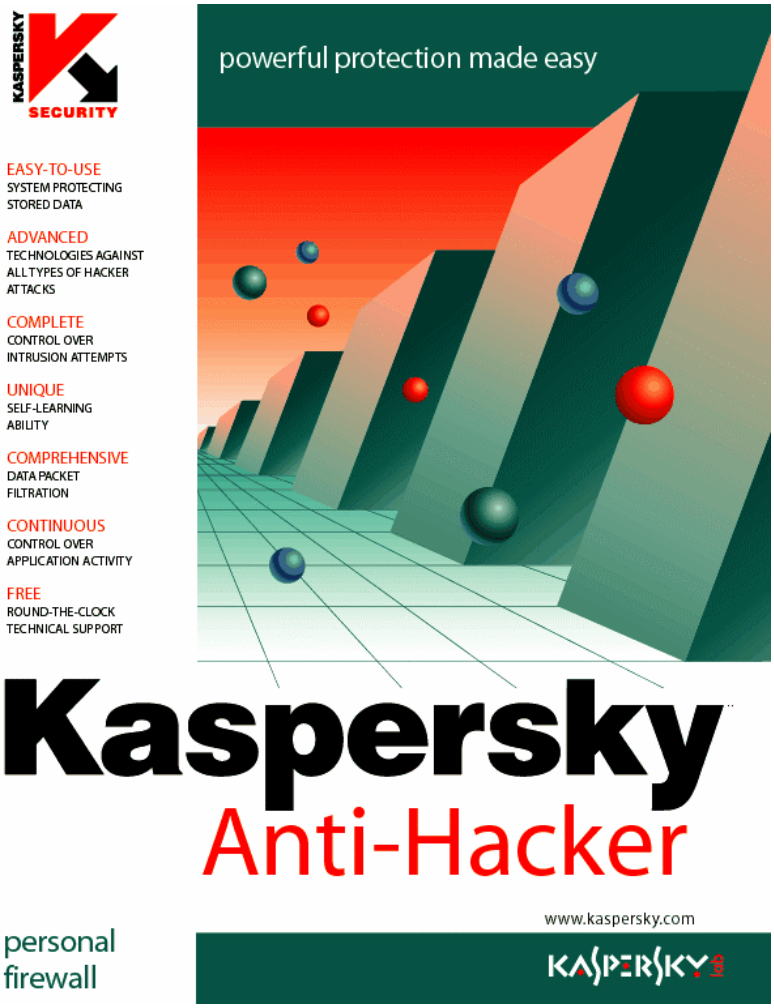
KASPERSKY LAB



Kaspersky Anti-Hacker 1.7

BENUTZERHANDBUCH

KASPERSKY ANTI-HACKER 1.7

Benutzerhandbuch

© Kaspersky Lab
http://www.kaspersky.com/de/

Redaktion: November 2004

Inhalt

KAPITEL 1. KASPERSKY ANTI-HACKER 5
1.1. Anwendungsbereich und Grundfunktionen des Programms 5
1.2. Was ist neu in Version 1.7 6
1.3. Lieferumfang 7
1.4. Inhalt des Benutzerhandbuchs 7
1.5. Textformatierung mit besonderer Bedeutung 9
1.6. Service für registrierte Benutzer 10

KAPITEL 2. INSTALLATION UND DEINSTALLATION DES PROGRAMMS 11
2.1. Soft- und Hardwarevoraussetzungen 11
2.2. Installation des Programms 12
2.3. Installation des Lizenzschlüssels 15
2.4. Deinstallation des Programms 15

KAPITEL 3. ERSTE SCHRITTE 17

KAPITEL 4. PRÄVENTION VON HACKER-ANGRIFFEN BEI DER ARBEIT IM INTERNET UND IN LOKALEN NETZWERKEN 20
4.1. Funktionsprinzipien von Kaspersky Anti-Hacker 20
4.2. Sicherheitsstufen 21
4.3. Konfigurationstipps 23

KAPITEL 5. PROGRAMMSTART UND BENUTZEROBERFLÄCHE 26
5.1. Programmstart 26
5.2. Systemmenü 27
5.3. Hauptfenster 28
5.3.1. Menü 29
5.3.2. Symbolleiste 31

5.3.3. Arbeitsbereich 33
5.3.4. Statusleiste 33
5.4. Kontextmenü der Dialogfenster 34
5.5. Assistent zur Regelerstellung 34
5.6. Ändern und Speichern von Eigenschaften der Benutzeroberfläche 34
5.7. Beenden des Programms 37

KAPITEL 6. AKTIVIERUNG UND EINSTELLUNGEN DES SCHUTZES 38
6.1. Aktivierung des Schutzes und Wahl der Sicherheitsstufe 38
6.1.1. Aktivierung des Schutzes 38
6.1.2. Auswahl der Sicherheitsstufe 40
6.1.3. Hinweis auf ein Netzwerk-Ereignis 41
6.1.4. Konfigurationsfenster 42
6.1.5. Warnung über Veränderung eines ausführbaren Moduls 44
6.2. Programmaktionen bei einem Angriff 45
6.3. Konfiguration der Regeln für Anwendungen 46
6.3.1. Arbeit mit der Regelliste 46
6.3.2. Hinzufügen einer neuen Regel 49
6.3.2.1. Schritt 1. Konfiguration der Regel 50
6.3.2.2. Schritt 2. Bedingungen für die Anwendung der Regel 54
6.3.2.3. Schritt 3. Angabe der zusätzlichen Aktionen 59
6.4. Konfiguration der Regeln für Paketfilterung 60
6.4.1. Arbeit mit der Regelliste 60
6.4.2. Hinzufügen einer neuen Regel 63
6.4.2.1. Schritt 1. Angabe der Bedingungen für die Anwendung der Regel 63
6.4.2.2. Schritt 2. Angabe eines Namens für die Regel und zusätzlicher Aktionen 68
6.5. Angriffsdetektor 69
6.5.1. Konfigurationsfenster des Angriffsdetektors 69
6.5.2. Liste der feststellbaren Hackerangriffe 70

KAPITEL 7. ANSICHT DER ARBEITSERGEBNISSE 73

7.1. Informationen über den aktuellen Status 73
7.1.1. Liste der aktiven Anwendungen 73
7.1.2. Liste der aktiven Verbindungen 77
7.1.3. Liste der offenen Ports 80
7.2. Arbeit mit den Protokollen 82
7.2.1. Öffnen des Protokollfensters 83
7.2.2. Benutzeroberfläche des Protokollfensters 83
7.2.2.1. Hauptmenü 84
7.2.2.2. Protokolltabelle 84
7.2.2.3. Verknüpfungen mit den Registerkarten 85
7.2.3. Auswahl des Protokolls 85
7.2.3.1. Das Protokoll "Sicherheit" 85
7.2.3.2. Das Protokoll "Aktivität der Anwendungen" 86
7.2.3.3. Das Protokoll "Paketfilterung" 87
7.2.4. Konfiguration der Protokollparameter 88
7.2.5. Speichern einer Protokolldatei auf der Festplatte 89
A.1. Andere Produkte von Kaspersky Lab 91
A.2. Kontaktinformationen 96

KAPITEL 1. KASPERSKY ANTI-HACKER

1.1. Anwendungsbereich und Grundfunktionen des Programms

Das Programm Kaspersky Anti-Hacker ist eine Personal Firewall und dient dem Schutz eines Computers, der mit dem Betriebssystem Windows arbeitet, vor unberechtigtem Zugriff auf Daten, sowie vor Netzwerk-Hackerangriffen aus einem lokalen Netzwerk oder aus dem Internet.

Das Programm Kaspersky Anti-Hacker erfüllt folgende Funktionen:

- Es verfolgt die Netzwerk-Aktivität nach dem Protokoll TCP/IP aller Anwendungen auf Ihrem Computer. Werden verdächtige Aktionen einer bestimmten Anwendung erkannt, dann werden Sie vom Programm darüber informiert und nötigenfalls wird der Netzwerk-Zugriff für diese Anwendung blockiert. Dadurch wird die Sicherheit der Daten, die auf Ihrem Computer gespeichert sind, garantiert. Wenn zum Beispiel ein "trojanisches" Programm versucht, Ihre Daten über das Internet an unberechtigte Dritte weiterzugeben, blockiert Kaspersky Anti-Hacker dessen Netzwerk-Zugriff.

- Die SmartStealth™ Technologie erschwert es, den Computer von außen zu erkennen. Dadurch verlieren Hacker ihr Angriffsobjekt und jeder Versuch, Zugriff auf den Computer zu erhalten, ist zum Scheitern verurteilt. Außerdem können auf diese Weise alle Arten von DoS (Denial of Service) Angriffen verhindert werden. Dabei übt der Tarnmodus keinerlei negativen Einfluss auf Ihre Arbeit im Internet aus: Das Programm gewährleistet die gewohnte Übersicht und den Datenzugriff.

- Es blockiert die verbreiteten Netzwerk-Hackerangriffe durch die kontinuierliche Filterung des eingehenden und ausgehenden Traffic und informiert den Benutzer darüber.

- Es verfolgt Versuche zum Scannen von Ports (die gewöhnlich Netzwerk-Angriffen vorausgehen) und blockiert den weiteren Datenaustausch mit einem angreifenden Computer.

- Es erlaubt die Ansicht einer Liste aller bestehenden Verbindungen, offenen Ports und aktiven Internet-Anwendungen. Nötigenfalls können unerwünschte Verbindungen getrennt werden.

- Es erlaubt die Arbeit mit dem Programm, ohne eine spezielle Konfiguration vorzunehmen. Das Programm unterstützt die vereinfachte Administration mit fünf Sicherheitsstufen: Alle erlauben, Niedrig, Mittel, Hoch, Alle blockieren. Als Standardeinstellung gilt die mittlere Sicherheitsstufe (Mittel), in der das Sicherheitssystem in Abhängigkeit von den Reaktionen des Benutzers auf verschiedene Ereignisse kontinuierlich konfiguriert wird.

- Es erlaubt bei Bedarf die flexible Konfiguration des Schutzsystems. Insbesondere erlaubt es die Konfiguration des Filtersystems für erwünschte und unerwünschte Netzwerk-Operationen und die Konfiguration des Angriffsdetektors.

- Es erlaubt die Aufzeichnung bestimmter, mit der Netzwerksicherheit verbundener Ereignisse in speziellen Protokollen. Die Ausführlichkeit der Ereignisaufzeichnungen im Protokoll kann nach Wunsch angepasst werden.

Das Programm kann als Einzelprodukt verwendet oder in unterschiedliche integrierte Lösungen von **Kaspersky Lab** aufgenommen werden.

Vorsicht!!! Kaspersky Anti-Hacker schützt Ihren Computer nicht vor Viren und schädlichen Programmen, die Ihre Daten vernichten oder beschädigen können. Für den Antivirenschutz Ihres Computers empfehlen wir die Verwendung von Kaspersky Anti-Virus® Personal.

1.2. Was ist neu in Version 1.7

Die neue Programmversion unterstützt abweichend von der Version 1.5 das Service Pack 2 für das Betriebssystem Windows XP.

1.3. Lieferumfang

Der Lieferumfang des Softwareprodukts umfasst folgende Komponenten:

- Versiegelter Umschlag mit der Installations-CD, auf der die Dateien des Softwareprodukts gespeichert sind
- Benutzerhandbuch
- Schlüssel-Diskette oder auf der Installations-CD gespeicherte Schlüssel-Datei
- Lizenzvertrag

Bitte lesen Sie vor dem Öffnen des versiegelten Umschlags mit der Installations-CD (oder mit den Disketten) sorgfältig den Lizenzvertrag.

Der Lizenzvertrag ist eine rechtliche Vereinbarung zwischen Ihnen und Kaspersky Lab. In diesem Vertrag wird festgelegt, zu welchen Bedingungen Sie das von Ihnen erworbene Softwareprodukt verwenden dürfen.

Bitte lesen Sie den Lizenzvertrag sorgfältig!

Wenn Sie den Bedingungen des Lizenzvertrags nicht zustimmen, können Sie die Packung mit Kaspersky Anti-Hacker an den Händler zurückgeben, bei dem Sie diese erworben haben, und der Kaufbetrag des Abonnements wird an Sie zurückerstattet. Voraussetzung dafür ist, dass der Umschlag mit der Installations-CD (oder mit den Disketten) nicht geöffnet wurde.

Durch das Öffnen der versiegelten Packung mit der Installations-CD (oder mit den Disketten) stimmen Sie allen Bedingungen des Lizenzvertrags zu.

1.4. Inhalt des Benutzerhandbuchs

Diese Dokumentation enthält die für Installation, Konfiguration und Benutzung des Programms Kaspersky Anti-Hacker notwendigen Informationen.

Die Dokumentation besteht aus folgenden Kapiteln:

Kapitel	**Kurzbeschreibung**
Kaspersky Anti-Hacker	Grundlegende Produktinformationen, Beschreibung des Lieferumfangs und der Struktur des Handbuchs
Installation und Deinstallation des Programms	Notwendige Systemvoraussetzungen. Beschreibung des Vorgehens zur Installation und Deinstallation
Erste Schritte	Anfangsphase der Arbeit mit dem Programm. Beispiel für die Konfiguration des Schutzsystems
Prävention von Hackerangriffen bei der Arbeit im Internet und in lokalen Netzwerken	Funktionsprinzipien des Softwareprodukts. Grundlegende Terminologie und Beschreibung der möglichen Hauptaufgaben
Programmstart und Benutzeroberfläche	Öffnen des Hauptfensters und Benutzeroberfläche des Programms
Aktivierung und Einstellungen des Schutzes	Aktivieren des Schutzes. Konfiguration der Schutzeinstellungen: Regeln für Anwendungen und Regeln für Paketfilterung
Ansicht der Arbeitsergebnisse	Anzeige der Protokolle über Sicherheit, Anwendungsaktivität und Paketfilterung. Anzeige der Liste der offenen Ports, bestehenden Verbindungen und aktiven Netzwerk-Anwendungen
Anhang A. Kaspersky Lab	Informationen über Kaspersky Lab Kontaktinformationen
Anhang B. Index	Glossar der im Benutzerhandbuch verwendeten Begriffe
Anhang C. Häufige Fragen	Antworten auf Fragen, die häufig von Anwendern gestellt werden

1.5. Textformatierung mit besonderer Bedeutung

Bestimmte Textteile dieser Dokumentation sind in Abhängigkeit ihrer Bedeutung durch unterschiedliche Formatierungselemente markiert. In der folgenden Tabelle werden die verwendeten Textformatierungen mit besonderer Bedeutung erläutert.

Formatierung	Bedeutung
Fette Schrift	Namen von Menüs, Menüpunkten, Fenstern, Elementen von Dialogfenstern usw.
Hinweis.	Zusatzinformationen, Bemerkungen.
Vorsicht	Sehr wichtige Information.
Um das Programm zu starten, führen Sie folgende Aktionen durch: 1. Schritt 1. 2. …	Beschreibung einer Reihe von auszuführenden Schritten und möglichen Aktionen.
Aufgabe:	Mögliche Aufgabenstellung als Beispiel für die Realisierung von Einstellungen, Funktionen usw.
Lösung	Lösung der Aufgabe.

1.6. Service für registrierte Benutzer

Kaspersky Lab bietet seinen registrierten Kunden ein breites Spektrum an Serviceleistungen, die eine gesteigerte Effektivität von Kaspersky Anti-Hacker ermöglichen.

Durch den Erwerb eines Abonnements werden Sie zum registrierten Programmbenutzer und können während der Gültigkeitsdauer Ihres Abonnements folgende Serviceleistungen in Anspruch nehmen:

- Nutzung neuer Versionen des betreffenden Softwareprodukts
- Beratung bei Fragen zu Installation, Konfiguration und Benutzung des Softwareprodukts (per Telefon und E-Mail)
- Nachrichten über das Erscheinen neuer Softwareprodukte von Kaspersky Lab und über das Auftauchen neuer Viren (dieser Service gilt für Benutzer, die den Newsletter von Kaspersky Lab abonniert haben).

Die Beratung bezieht sich nicht auf Fragen über Funktion und Benutzung von Betriebssystemen und anderen Technologien.

KAPITEL 2. INSTALLATION UND DEINSTALLATION DES PROGRAMMS

2.1. Soft- und Hardwarevoraussetzungen

Für die Funktion von **Kaspersky Anti-Hacker** sind folgende Soft- und Hardwarevoraussetzungen erforderlich:

Allgemeine Voraussetzungen:

- Computer mit installiertem Betriebssystem Microsoft Windows Version 98/ME/NT 4.0/2000/XP
- für Microsoft Windows Version NT 4.0/2000/XP sind Administratorenrechte notwendig
- Unterstützung des Protokolls TCP/IP
- lokales Netzwerk (Ethernet) oder Modemverbindung (Standard oder mit ADSL-Modem)
- Microsoft Internet Explorer Version 5.0 oder höher
- mindestens 50 MB freier Speicherplatz auf der Festplatte für Programmdateien, sowie Platz zum Speichern von Protokollen im gewünschten Umfang

Bei der Arbeit mit dem Betriebssystem Windows® 98/Me/NT 4.0 sind erforderlich:

- Intel Pentium® 133MHz oder höher für Windows 98 und Windows NT 4.0
- Intel Pentium® 150MHz oder höher für Windows ME

- 32 MB RAM Arbeitsspeicher
- für Windows NT 4.0 Workstation das installierte Service Pack Version 6.0 oder höher

Bei der Arbeit mit dem Betriebssystem Windows 2000 sind erforderlich:

- Intel Pentium 133MHz oder höher
- 64 MB RAM Arbeitsspeicher

Bei der Arbeit mit dem Betriebssystem Windows XP sind erforderlich:

- Intel Pentium 300MHz oder höher
- 128 MB RAM Arbeitsspeicher

2.2. Installation des Programms

Starten Sie zur Installation des Softwareprodukts auf der CD-ROM das Programm Setup.exe. Das Installationsprogramm funktioniert im Dialogmodus. Jedes Dialogfenster enthält eine bestimmte Auswahl von Schaltflächen zur Steuerung des Installationsprozesses. Hier eine kurze Erklärung der wichtigsten Schaltflächentypen und deren Funktion:

- **OK** – Aktionen akzeptieren
- **Abbrechen** – Aktionen abbrechen
- **Weiter** – einen Schritt weitergehen
- **Zurück** – einen Schritt zurückgehen

Vor der Installation des Programms Kaspersky Anti-Hacker sollten alle auf dem Computer geöffneten Programme beendet werden.

Schritt 1. Startfenster für Installationsvorgang

Nach Ausführen der Datei *setup.exe* wird auf dem Bildschirm das Startfenster geöffnet, in dem Angaben zum Aufruf der Programminstallation von Kaspersky Anti-Hacker auf Ihrem Computer stehen.

Zur Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter >**. Zum Ablehnen der Installation klicken Sie auf die Schaltfläche **Abbrechen**.

Schritt 2. Lesen des Lizenzvertrags

Das folgende Fenster enthält den Text des Lizenzvertrags zwischen Ihnen und Kaspersky Lab. Bitte lesen Sie sich den Vertrag sorgfältig durch. Wenn Sie den Bedingungen des Lizenzvertrags in allen Punkten zustimmen, klicken Sie auf die Schaltfläche **Akzeptieren**. Der Installationsvorgang geht weiter.

Schritt 3. Angabe der Benutzerinformationen

In diesem Schritt der Installation werden der Benutzername und der Name der Organisation abgefragt. Als Standard sind die Angaben vorgegeben, die in der Registry des Betriebssystems hinterlegt sind. Sie können die Werte überschreiben.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter >**.

Schritt 4. Installation des Lizenzschlüssels

In diesem Schritt der Installation wird der Lizenzschlüssel von Kaspersky Anti-Hacker installiert. Der Lizenzschlüssel ist Ihr „persönlicher Schlüssel“, in dem alle Serviceangaben gespeichert sind, die für eine vollständige Funktionalität des Programms benötigt werden sowie der Name und die Nummer der Lizenz sowie deren Ablaufdatum.

Das Programm funktioniert nicht ohne Lizenzschlüssel.

Im Standardfenster Datei auswählen geben Sie den Lizenzschlüssel ein und klicken Sie auf die Schaltfläche **Weiter >**, um den Installationsvorgang fortzusetzen.

Sollten Sie bei der Installation den Lizenzschlüssel nicht zur Hand haben (Sie haben beispielsweise bei Kaspersky Lab im Internet bestellt, den Schlüssel aber noch nicht erhalten), können Sie ihn später nachinstallieren. Beachten Sie, dass Sie mit Kaspersky Anti-Hacker aber noch nicht arbeiten können.

Schritt 5. Auswahl des Installationsordners

Im folgenden Installationsschritt informieren Sie Kaspersky Anti-Hacker über den Zielordner auf Ihrem Computer, wohin das Programm installiert werden soll. Als Standard gilt der folgende Pfad: **Program Files\Kaspersky Lab\Kaspersky Anti-Hacker**.

Um den Pfad zu ändern, klicken Sie auf die Schaltfläche **Durchsuchen…**, im Standardfenster geben Sie den Installationsordner für die Software ein und klicken auf die Schaltfläche **Weiter >**.

Danach erfolgt das Kopieren der Dateien von Kaspersky Anti-Hacker auf Ihren Computer.

Schritt 6. Kopieren der Dateien auf die Festplatte

Im Dialogfenster Kopieren der Dateien können Sie den Fortschritt für das Kopieren der Dateien auf die Festplatte des Computers verfolgen.

Schritt 7. Abschluss der Installation

Das Fenster Abschluss der Installation enthält Angaben über den Abschluss der Installation von Kaspersky Anti-Hacker auf Ihrem Computer.

Wenn zum Abschluss des Installationsprozesses eine Reihe von Services im System registriert werden müssen, wird Ihnen der Neustart des Computers vorgeschlagen. Für eine korrekte Installation MÜSSEN Sie das tun.

Um die Installation des Programms abzuschließen,

1. wählen Sie aus den folgenden Varianten aus:

   - **Ja. Rechner jetzt neu starten**
   - **Nein. Rechner später neu starten**

2. Klicken Sie auf die Schaltfläche **Fertigstellen**.

2.3. Installation des Lizenzschlüssels

Falls bei der Installation von Kaspersky Anti-Hacker noch kein Lizenzschlüssel installiert worden ist, funktioniert das Programm nicht.

Um die Funktionen des Programms nutzen zu können, muss ein Lizenzschlüssel installiert werden.

Zur Installation des Lizenzschlüssels führen Sie die folgenden Aktionen aus:

Klicken Sie mit der Maus doppelt auf die Datei des Lizenzschlüssels. Es erfolgt eine automatische Installation.

oder

Kopieren Sie die Datei mit dem Lizenzschlüssel in den Ordner **Program Files\Common Files\Kaspersky Lab**.

2.4. Deinstallation des Programms

Zur Deinstallation des Programms Kaspersky Anti-Hacker gehen Sie folgendermaßen vor:

Klicken Sie in der Windows-Taskleiste auf die Schaltfläche **Start** und wählen Sie im folgenden Windows-Menü den Punkt **Programme → Kaspersky Anti-Hacker → Kaspersky Anti-Hacker deinstallieren**.

Es öffnet sich daraufhin der Assistent für die Deinstallation.

Schritt 1. Startfenster für Deinstallationsvorgang

Dieses Fenster informiert Sie über das Aufrufen der Deinstallation von Kaspersky Anti-Hacker von Ihrem Computer. Zum Fortsetzen klicken Sie auf die Schaltfläche **Weiter**.

Schritt 2. Deinstallation des Programms vom Computer

In diesem Dialogfenster wird der Ordner angezeigt, aus dem das Programm gelöscht wird. Klicken Sie auf die Schaltfläche **Löschen**, um die Deinstallation von Kaspersky Anti-Hacker von Ihrem Computer einzuleiten. Der Deinstallationsvorgang für die Programmdateien wird im Fenster des Deinstallationsassistenten angezeigt.

Schritt 3. Abschluss des Deinstallationsvorganges

Das Fenster **Abschluss der Deinstallation** enthält Angaben über den Abschluss des Deinstallationsvorganges von Kaspersky Anti-Hacker. Für eine korrekte Deinstallation muss Ihr Computer neu gestartet werden.

Um die Deinstallation des Programms abzuschließen,

1. wählen Sie aus den folgenden Varianten aus:
   - **Ja. Rechner jetzt neu starten**
   - **Nein. Rechner später neu starten**
2. Klicken Sie auf die Schaltfläche **Fertigstellen**.

Das Programm kann auch im Fenster **Programme ändern und entfernen** entfernt werden, das über die **Systemsteuerung** aufgerufen wird.

KAPITEL 3. ERSTE SCHRITTE

Nach der Installation des Programms und dem Neustart Ihres Computers tritt das Sicherheitssystem in Aktion. Faktisch verfolgt Kaspersky Anti-Hacker genau ab diesem Moment Angriffe auf Ihren Computer sowie Versuche zum Datenaustausch von Anwendungen mit einem lokalen Netzwerk oder mit dem Internet.

Nach der Anmeldung am System beginnen Sie wie üblich zu arbeiten. Findet kein Datenaustausch über ein Netzwerk statt, dann informiert lediglich das Verknüpfungssymbol im Infobereich der Taskleiste über die Gegenwart des Programms auf dem Computer. Durch Klick auf das Symbol können Sie das Hauptfenster des Programms öffnen, Informationen über die aktuelle Sicherheitsstufe erhalten und die Sicherheitsstufe ändern (das Hauptfenster wird ausführlich in Pkt. 5.3 auf S. 28 beschrieben). In der Standardeinstellung arbeitet das Programm mit der Sicherheitsstufe **Mittel**, die Ihnen erlaubt, das Schutzsystem auf einfache Weise zu konfigurieren. Gewöhnlich ist es nicht erforderlich, das Programm selbst zu konfigurieren: Den Anwendungen, die am häufigsten verwendet werden, wird in Übereinstimmung mit ihrem Typ standardmäßig die Netzwerk-Aktivität erlaubt. Trotzdem kann in bestimmten Situationen die manuelle Konfiguration notwendig sein. Betrachten wir diesen Prozess genauer.

Aufgabe. Nehmen wir an, Ihr Computer ist mit dem Internet verbunden. Sie haben Microsoft Internet Explorer gestartet und die Adresse der Seite www.kaspersky.com eingegeben. Daraufhin erscheint auf dem Bildschirm Ihres Computers das Dialogfenster **Regel erstellen für IEXPLORER.EXE** (s. Abb. 1).

Der obere Bereich des Fensters enthält folgende Elemente: das Programmsymbol und den Namen von Microsoft Internet Explorer, die Adresse der Internetseite www.kaspersky.com und die Nummer des Ports, der für den Verbindungsaufbau verwendet wird. Ausführliche Informationen über die Verbindung können Sie durch Klick auf den unterstrichenen Link erhalten (s. Abb. 2).

Bevor Sie nicht angeben, wie das Programm verfahren soll, kann keine Netzwerk-Verbindung aufgebaut werden. Ihre Reaktion auf den vom Programm ausgegebenen Hinweis ist erforderlich.

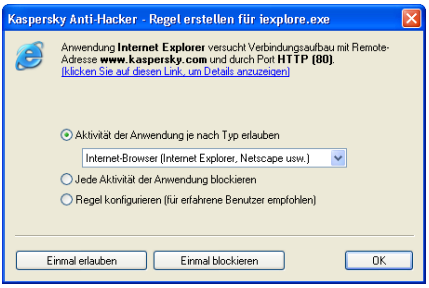

Kaspersky Anti-Hacker - Regel erstellen für iexplore.exe
Anwendung Internet Explorer versucht Verbindungsaufbau mit Remote-Adresse www.kaspersky.com und durch Port HTTP (80).
[Klicken Sie auf diesen Link, um Details anzuzeigen]
Aktivität der Anwendung je nach Typ erlauben
Internet-Browser (Internet Explorer, Netscape usw.)
Jede Aktivität der Anwendung blockieren
Regel konfigurieren (für erfahrene Benutzer empfohlen)
Einmal erlauben
Einmal blockieren
OK

Abbildung 1. Konfigurationsfenster des Sicherheitssystems

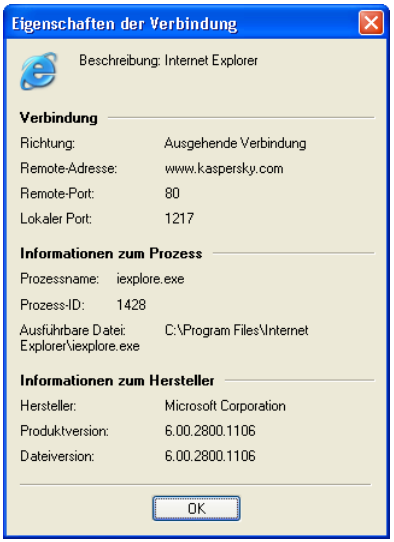


Abbildung 2. Eigenschaften der Verbindung

Gehen Sie folgendermaßen vor:

1. Wählen Sie die Schaltfläche **Aktivität dieser Anwendung je nach Typ erlauben** und wählen Sie in der darunter angebrachten Dropdown-Liste den Wert **Internet-Browser**.

2. Klicken Sie auf die Schaltfläche **OK**.

Danach erlaubt Kaspersky Anti-Hacker dem Programm Microsoft Internet Explorer den Verbindungsaufbau. Außerdem werden diesem Programm alle künftigen Verbindungen, die für einen Webbrowser üblich sind, erlaubt.

Wie Sie beim Lösen der Aufgabe bemerkt haben, stehen im Fenster **Regel erstellen für IEXPLORER.EXE** drei Aktionsvarianten zur Auswahl:

- **Aktivität dieser Anwendung je nach Typ erlauben** (diese Option wurde im Beispiel gewählt) – Der Anwendung, die das Ereignis hervorgerufen hat, wird jeder Netzwerk-Datenaustausch erlaubt, der mit dem Anwendungstyp übereinstimmt. Der Typ wird in der Dropdown-Liste

festgelegt, die sich unterhalb des Optionsfelds befindet. Sie können der Anwendung jede beliebige Aktivität erlauben, indem Sie den Wert **Alle erlauben** festlegen.

- **Jede Aktivität dieser Anwendung blockieren** – Für die Anwendung, die das Ereignis hervorgerufen hat, werden sowohl die aktuelle Operation, als auch alle anderen Netzwerk-Operationen in Zukunft blockiert.

- **Regel konfigurieren** – Der Anwendung werden die aktuelle Operation und alle gleichartigen Netzwerk-Operationen in Zukunft erlaubt. Die Bedingungen für die Netzwerk-Operationen werden nach dem Klick auf die Schaltfläche **OK** mit Hilfe des Regelassistenten festgelegt (Einzelheiten über den Assistenten s. Pkt. 6.3.2 auf S. 49)

Sollten Sie sich bei der Auswahl der Aktion nicht sicher sein, können Sie auf die Schaltfläche **Einmal erlauben** oder **Einmal blockieren** klicken und das weitere Verhalten der Anwendung beobachten, die versucht Netzwerk-Zugriff zu erhalten.

Wenn Sie das Konfigurationsfenster durch Klick auf die Schaltfläche in der oberen rechten Ecke schließen, wird die betreffende Operation ein Mal blockiert.

Auf diese Weise können sie im Verlauf der Arbeit das Sicherheitssystem Ihres Computers optimal einstellen.

Die Liste der erstellten Regeln können Sie durch die Auswahl des Punktes **Regeln für Anwendungen** im Menü **Service** oder durch Klick auf die Schaltfläche öffnen.

Für die ersten Wochen nach der Installation des Programms auf dem Computer empfehlen wir die Verwendung der Sicherheitsstufe **Mittel**. Während Sie wie gewohnt mit dem Netzwerk arbeiten, wird das Programm auf der Basis Ihrer Reaktionen auf bestimmte Netzwerk-Operationen konfiguriert und Regeln werden erstellt.

Nach der Konfigurationsphase können Sie auf die Sicherheitsstufe **Hoch** wechseln. Dadurch schützen Sie sich vor beliebigen nicht ausdrücklich erlaubten Netzwerk-Ereignissen und Hackerangriffen. Erinnern Sie sich aber daran, dass in dieser Stufe neu installierten Netzwerk-Anwendungen in der Grundeinstellung kein Zugriff auf das Internet gewährt wird. Zur Konfiguration von Kaspersky Anti-Hacker ist es in diesem Fall erforderlich, erneut auf die Stufe **Mittel** zu wechseln oder selbständig eine Regel für die neu installierten Anwendungen zu erstellen.

KAPITEL 4. PRÄVENTION VON HACKER-ANGRIFFEN BEI DER ARBEIT IM INTERNET UND IN LOKALEN NETZWERKEN

4.1. Funktionsprinzipien von Kaspersky Anti-Hacker

Kaspersky Anti-Hacker schützt Ihren Computer vor Netzwerk-Angriffen und garantiert außerdem die Sicherheit Ihrer Daten. Dazu kontrolliert Kaspersky Anti-Hacker alle Netzwerk-Operationen auf Ihrem Computer. Es werden zwei Typen von Netzwerk-Operationen unterschieden:

- Operationen auf der Anwendungsebene (in einer hohen Netzwerkschicht). Auf dieser Ebene analysiert Kaspersky Anti-Hacker die Aktivität solcher Anwendungen wie Webbrowser, E-Mail-Programme, Dateiübertragungsprogramme usw.

- Operationen auf der Paket-Ebene (in einer niedrigen Netzwerkschicht). Auf dieser Ebene analysiert Kaspersky Anti-Hacker unmittelbar die Pakete, die von Ihrer Netzwerkkarte oder Ihrem Modem gesendet/empfangen werden.

Die Arbeit mit Kaspersky Anti-Hacker wird durch die Definition von Filterregeln für Netzwerk-Operationen vorgenommen. Ein Teil der Filtervorgänge wird automatisch vom Angriffsdetektor durchgeführt, der das Scannen von Ports, DoS-Angriffe u.ä. erkennt, sowie einen Angreifer blockieren kann. Zusätzlich können Sie eigene Filterregeln für den verbesserten Schutz Ihres Computer erstellen.

Für jeden Typ der Netzwerk-Operationen sind in Kaspersky Anti-Hacker spezielle Regellisten vorhanden.

- *Regeln für Anwendungen*. Hier können Sie eine konkrete Anwendung wählen und eine spezifische Aktivität für diese erlauben. Bei Bedarf können Sie eine beliebige Anzahl von Regeln für jede Anwendung erstellen. Werden Netzwerk-Operationen bemerkt, die von einer durch Sie erstellten Regel abweichen, werden Sie gewarnt und können nötigenfalls unerwünschte Aktionen blockieren (im Modus **Mittel**). Die einfachste Methode, eine solche Regel zu erstellen, besteht im Festlegen des Typs, dem die betreffende Anwendung angehört (zur Liste und Beschreibung der Typen s. Pkt. 6.3.2.1 auf S. 50). Die zweite Methode besteht im Festlegen der zugelassenen Remote-Dienste und -Adressen für diese Anwendung.

- Die *Regeln für Paketfilterung* erlauben oder blockieren Netzwerk-Pakete, die von Ihrem Computer gesendet oder empfangen werden. Die Entscheidung wird auf der Basis einer Header-Analyse des Netzwerk-Pakets getroffen: verwendetes Protokoll, Nummer des Ports, IP-Adressen u.a. In den Regeln für Paketfilterung legen Sie Regeln fest, die generell für alle Anwendungen gelten. Wenn Sie zum Beispiel mit Hilfe einer Regel für Paketfilterung eine bestimmte IP-Adresse blockiert haben, werden für diese Adresse alle Netzwerk-Operationen vollständig blockiert.

Die Regeln für Paketfilterung besitzen eine höhere Priorität als die Regeln für Anwendungen: Die Filterregeln werden vom Programm zuerst angewandt. Haben Sie zum Beispiel eine Regel zum Blockieren aller eingehenden und ausgehenden Pakete erstellt, dann bleiben alle Regeln für Anwendungen unberücksichtigt.

4.2. Sicherheitsstufen

Das Programm bietet fünf Sicherheitsstufen zur Auswahl.

- **Alle erlauben** – Das Programm deaktiviert den Schutz Ihres Computers. Bei der Arbeit in diesem Modus wird jede Netzwerk-Aktivität erlaubt.

- **Niedrig** – Das Programm erlaubt die Netzwerk-Aktivität für alle Anwendungen, außer für die mit Hilfe der Anwendungsregeln eindeutig blockierten Anwendungen.

- **Mittel** – Das Programm benachrichtigt Sie über die Netzwerk-Aktivität von Anwendungen und erlaubt die optimale Konfiguration des Sicherheitssystems. Beim Versuch einer Anwendung, eine Netzwerk-Operation auszuführen, wird der Konfigurationsmechanismus aufgerufen. Auf dem Bildschirm werden Informationen über die Anwendung und Parameter der Netzwerk-Operation angezeigt. Auf der Basis dieser

Angaben werden Sie zu einer Entscheidung aufgefordert: einmaliges Erlauben oder Blockieren des aktuellen Ereignisses, vollständiges Blockieren der Aktivität dieser Anwendung, Erlauben der Anwendungsaktivität in Übereinstimmung mit dem Typ, oder Konfiguration zusätzlicher Parameter für den Netzwerk-Datenaustausch. Auf der Basis Ihrer Antwort kann das Programm eine Regel für die entsprechende Anwendung erstellen, die in Zukunft automatisch angewandt wird.

- **Hoch** – Das Programm erlaubt nur jenen Anwendungen den Netzwerk-Zugriff, die mit Hilfe der Regeln eindeutig festgelegt wurden. In diesem Modus wird das Konfigurationsfenster nicht angezeigt und alle unerwünschten Verbindungen werden abgelehnt.

Erinnern Sie sich daran, dass Netzwerk-Anwendungen, die nach der Auswahl dieser Sicherheitsstufe installiert werden, in der Grundeinstellung keinen Internet-Zugriff erhalten.

- **Alle blockieren** – Das Programm blockiert den Zugriff Ihres Computers auf das Netzwerk vollständig. Dieser Modus entspricht der physikalischen Trennung des Computers vom Internet und/oder vom lokalen Netzwerk.

In den Sicherheitsstufen **Hoch**, **Mittel** und **Niedrig** können Sie die Zusatzfunktion **Stealth-Modus** aktivieren (s. Pkt. 5.3.3 auf S. 33). In diesem Modus ist die durch den Benutzer initiierte Netzwerk-Aktivität erlaubt. Dagegen wird jede andere Aktivität (von außen initiierter Verbindungsaufbau mit Ihrem Computer, Test mit dem Dienstprogramm ping usw.) verboten, außer sie ist ausdrücklich durch Regeln zugelassen.
Praktisch bedeutet dies, dass Ihr Computer für die externe Umgebung "unsichtbar" wird. Hacker verlieren ihr Angriffsobjekt und jeder Versuch, Zugriff auf den Computer zu erhalten, ist zum Scheitern verurteilt. Außerdem hilft der Stealth-Modus dabei, alle Arten von DoS (Denial of Service) Angriffen zu verhindern.
Gleichzeitig übt der Tarnmodus keinerlei negativen Einfluss auf Ihre Arbeit im Internet aus: Kaspersky Anti-Hacker erlaubt die Netzwerk-Aktivität, die von Ihrem Computer initiiert wird.

Der Angriffsdetektor ist in allen Sicherheitsstufen aktiv, außer in der Stufe **Alle erlauben**. Es besteht aber die Möglichkeit, den Detektor zu deaktivieren (s. Pkt. 6.5.1 auf S. 69).

4.3. Konfigurationstipps

Welche Komponenten von Kaspersky Anti-Hacker sollen verwendet und welche Sicherheitsstufe soll gewählt werden? Die Antwort auf diese Fragen ist von der Aufgabe abhängig, die Sie zu lösen haben.

Aufgabe 1. Sie möchten Ihre Daten vor Angreifern aus dem Internet schützen.

Es bestehen zwei grundlegende Methoden zum Diebstahl oder zur Beschädigung von Daten auf dem Computer eines Benutzers durch Angreifer aus dem Internet: das Eindringen in den Computer über eine Schwachstelle in der Software und die Infektion des Computers durch trojanische Programme.

Wenn Sie von einem Fehler in einem bestimmten Programm erfahren haben, das auf Ihrem Computer installiert ist, erstellen Sie für dieses Programm eine Verbotsregel. Wir empfehlen Ihnen die Konfiguration einer komplexen Verbotsregel (s. Pkt. 6.3.2.1 auf S. 50), die alle Besonderheiten des Fehlers berücksichtigt.

Nehmen wir an, dass über eine Diskette oder über per E-Mail ein trojanisches Programm auf Ihren Computer gelangt ist und es versucht, Ihre Daten in das Internet zu schicken. Kaspersky Anti-Hacker gewährleistet problemlos die Sicherheit Ihrer Daten durch das Verbot dieser Operation (im Modus **Hoch**) oder durch die Ausgabe einer Warnung darüber (im Modus **Mittel**).

Vorsicht!!! Kaspersky Anti-Hacker schützt Ihren Computer nicht vor Viren und bietet keinen vollständigen Schutz vor schädlichen Programmen.

Zum Beispiel kann ein "trojanisches" Programm das Standard-E-Mail-Programm zum Senden Ihrer Daten verwenden, woran Kaspersky Anti-Hacker den Trojaner dann nicht hindern kann. Außerdem können, wenn ein Virus oder ein schädliches Programm auf Ihren Computer gelangt ist, Ihre Daten vernichtet werden oder der Computer kann zum Ausgangspunkt der Weiterverbreitung von Viren werden. Kaspersky Anti-Hacker kann in diesem Fall nur teilweise die Folgen einer Infektion verhindern. Für den effektiven Schutz vor Viren und schädlichen Programmen empfehlen wir die gleichzeitige Verwendung von Kaspersky Anti-Hacker und des Antiviren-Programms Kaspersky Anti-Virus® Personal / Personal Pro. Zusätzlich empfehlen wir, den Anwendungen in der Liste der Anwendungsregeln jene Kategorien zuzuweisen, die genau mit den Operationen übereinstimmen, deren Ausführung diesen Anwendungen erlaubt ist. Dadurch wird das Risiko der Ausführung unerwünschter Netzwerk-Operationen auf Ihrem Computer minimiert.

Nehmen wir an, Sie haben entdeckt, dass von bestimmten Remote-Computern ständig versucht wird, Ihren Computer anzugreifen.

Aufgabe 2. Verdächtige Internetadressen sollen blockiert werden.

Sie können den Datenaustausch Ihres Computers mit Remote-Adressen verbieten, indem Sie entsprechende Regeln für die Paketfilterung erstellen. Auf Abb. 3 ist als Beispiel eine Regel dargestellt, die das vollständige Blockieren der Adresse "111.111.111.111" erlaubt.

Zur Prophylaxe wird empfohlen, den Angriffsdetektor – unabhängig von der verwendeten Sicherheitsstufe – nie zu deaktivieren.

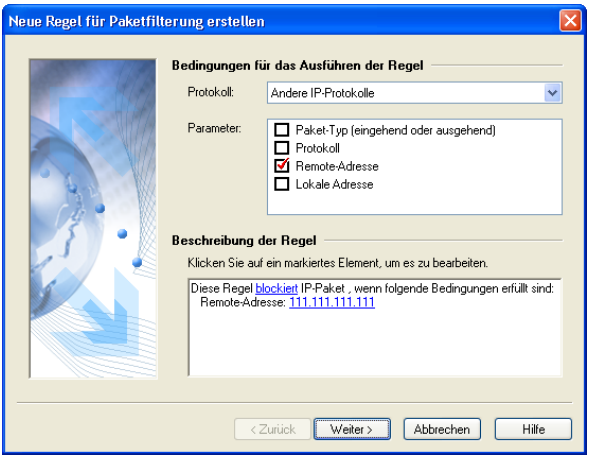


Abbildung 3. Regel für das Blockieren einer verdächtigen Adresse

Als interessantes Beispiel für die Verwendung des Programms Kaspersky Anti-Hacker kann das Blockieren der Anzeige von Bannern auf Webseiten dienen. Geben Sie in den Regeln für Paketfilterung das Verbot der Verbindung mit Internetseiten an, von denen Banner geladen werden (z.B. **tauschbanner.de**).

Nehmen wir an, Sie möchten sich vor Angriffen aus einem lokalen Netzwerk oder vor dem Diebstahl persönlicher Daten schützen.

Aufgabe 3. Kontrolle der Operationen des lokalen Netzwerks

Der Datenaustausch eines Computers mit dem lokalen Netzwerk findet auf Betriebssystemebene statt und es ist nicht immer möglich, die betreffende Anwendung zu benennen. Zur Gewährleistung der Sicherheit ist in diesem Fall das Festlegen von Regeln für die Paketfilterung erforderlich.

Das Programm Kaspersky Anti-Hacker erstellt für die Paketfilterung von sich aus bestimmte Erlaubnisregeln, um die Konfiguration des Sicherheitssystems zu vereinfachen. In der Grundeinstellung ist das lokale Netzwerk zugelassen. Sie können selbständig Änderungen der voreingestellten Regeln für die Paketfilterung vornehmen, um den Zugriff aus dem lokalen Netzwerk entweder vollständig zu blockieren oder den Zugriff nur für bestimmte Computer zuzulassen.

KAPITEL 5.
PROGRAMMSTART UND BENUTZEROBERFLÄCHE

5.1. Programmstart

Nach der Anmeldung am System wird Kaspersky Anti-Hacker automatisch gestartet. Wenn Sie das Programm beendet haben, können Sie es erneut manuell starten.

Zum Start des Programms Kaspersky Anti-Hacker

1. Klicken Sie in der Windows-Taskleiste auf die Schaltfläche **Start** und wählen Sie im folgenden Windows-Menü den Punkt **Programme → Kaspersky Anti-Hacker → Kaspersky Anti-Hacker**.

2. Klicken Sie in dem eingeblendeten Aufgabenfenster mit der linken Maustaste auf das Symbol oder mit der rechten Maustaste und wählen Sie im Kontextmenü des Programms den Punkt **Kaspersky Anti-Hacker öffnen** aus.

Dann erscheint das Hauptfenster des Programms Kaspersky Anti-Hacker auf dem Bildschirm (s. Pkt. 5.3 auf S. 28).

Sie können das Programm außerdem direkt aus dem Ordner starten, in den es installiert wurde. Öffnen Sie dazu im Windows Explorer den Ordner des Programms Kaspersky Anti-Hacker (als Standard **C:\Programme\Kaspersky Lab\Kaspersky Anti-Hacker**). Doppelklicken Sie auf das Verknüpfungssymbol der Datei ***KAVPF.exe***.

5.2. Systemmenü

Nach dem Programmstart erscheint im Infobereich der Taskleiste das Verknüpfungssymbol .

Durch Rechtsklick auf das Programmsymbol können Sie das Kontextmenü öffnen (s. Abb. 4). Es besteht aus den folgenden Punkten:

Tabelle 1

Menüpunkt	Funktion
Kaspersky Anti-Hacker öffnen…	Öffnen des Programmhauptfensters.
Sicherheitsstufe	Auswahl der Sicherheitsstufe: **Alle blockieren**, **Hoch**, **Mittel**, **Niedrig**, **Alle erlauben**. Einzelheiten zu den Sicherheitsstufen s. Pkt. 4.2 auf S. 21.
Über das Programm...	Öffnen des Fensters mit Informationen über die Programmversion und über verwendete Schlüssel.
Beenden	Entfernen des Programms aus dem Arbeitsspeicher

Abbildung 4. Das Kontextmenü

5.3. Hauptfenster

Nach dem Programmstart wird auf dem Bildschirm das Hauptfenster des Programms geöffnet (s. Abb. 5). Das Hauptfenster des Programms Kaspersky Anti-Hacker dient der Auswahl der aktuellen Sicherheitsstufe, der Anzeige des aktuellen Schutzstatus, der Änderung von Einstellungen für Paketfilterung und der Ansicht/Konfiguration der Protokolle.

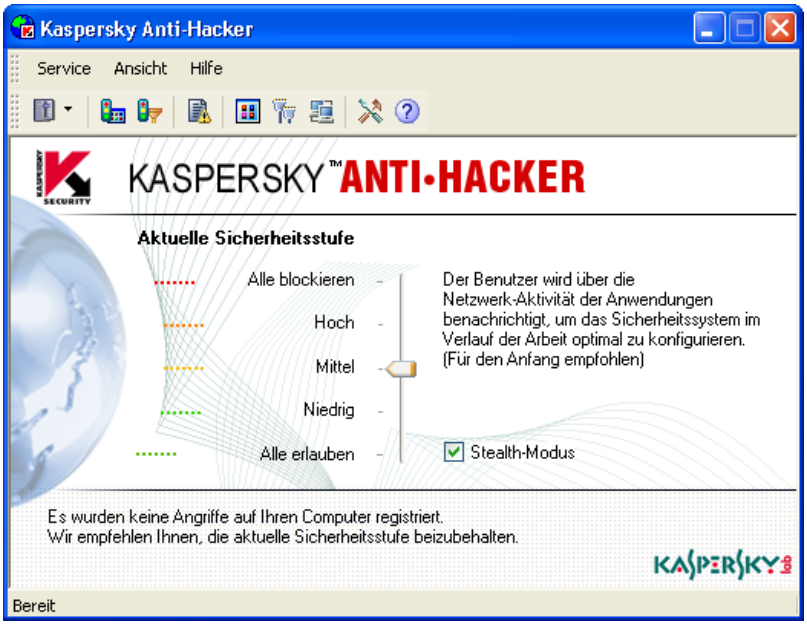


Abbildung 5. Das Hauptfenster von **Kaspersky Anti-Hacker**

Das Hauptfenster des Programms Kaspersky Anti-Hacker besteht aus folgenden Elementen:

- Menü
- Symbolleiste
- Arbeitsbereich
- Statusleiste

5.3.1. Menü

Im oberen Bereich des Hauptfensters befindet sich das *Menü*. Sie können das Menü an jedem beliebigen Ort innerhalb oder außerhalb des Programmfensters platzieren, indem Sie es mit der Maus verschieben.

Bestimmte Menüpunkte besitzen analoge Schaltflächen auf der Symbolleiste. Die Entsprechung von Schaltflächen auf der Symbolleiste und Menüpunkten wird in Pkt. 5.3.2 auf S. 31 dargestellt.

Tabelle 2

Menüpunkt	**Funktion**
Service ⟶ Regeln für Anwendungen	Öffnen des Konfigurationsfensters für die Anwendungsregeln.
Service ⟶ Regeln für Paketfilterung	Öffnen des Konfigurationsfensters für die Paketfilterungsregeln.
Service ⟶ Sicherheitsstufe	Auswahl der Sicherheitsstufe: • Alle blockieren • Hoch • Mittel • Niedrig • Alle erlauben Die Sicherheitsstufe kann auch im Arbeitsbereich des Programms gewählt werden. Zu Details s. Pkt. 4.2 auf S. 21.
Service⟶ Einstellungen	Öffnen des Konfigurationsfensters für Protokolleinstellungen, Einstellungen für die Aktivierung des Schutzes und Einstellungen des Angriffsdetektors.

Menüpunkt	**Funktion**
Service ⟶ Beenden	Entfernen des Programms aus dem Arbeitsspeicher.
Ansicht ⟶ Symbolleisten	Konfigurieren der Programmoberfläche: • **Standard-Symbolleiste** – Symbolleiste einblenden/ausblenden • **Anpassen** – Öffnen des Dialogfensters zur Konfiguration der Programmoberfläche.
Ansicht ⟶ Statusleiste	Statusleiste einblenden / ausblenden.
Ansicht ⟶ Protokolle	Öffnen des Fensters mit den Protokollen für: • **Sicherheit** • **Aktivität der Anwendungen** • **Paketfilterung**.
Ansicht ⟶ Anzeigen	Öffnen des Fensters zur Anzeige von Systeminformationen: • **Aktive Anwendungen** – Liste der gestarteten Netzwerk-Anwendungen • **Offene Ports** – Liste der offenen Ports • **Aktive Verbindungen** – Liste der aktiven Verbindungen.
Hilfe ⟶ Inhalt	Aufruf des Hilfesystems.

Menüpunkt	Funktion
Hilfe ⟶ Über das Programm...	Öffnen des Dialogfensters mit Kurzinformationen über Programmversion und verwendete Schlüssel.
Hilfe ⟶ Kaspersky Anti-Hacker im Internet	Öffnen der Webseite von Kaspersky Lab

5.3.2. Symbolleiste

Die Symbolleiste befindet sich unter der Menüzeile. Sie kann innerhalb oder außerhalb des Hauptfensters platziert werden. Verschieben Sie dazu die Symbolleiste mit der Maus.

Auf der *Symbolleiste* befinden sich Schaltflächen, durch deren Anklicken bestimmte Aktionen ausgeführt werden können. Durch die Auswahl des Punktes **Symbolleisten** im Menü **Ansicht** und Klick auf den Punkt **Standard-Symbolleiste** im folgenden Untermenü kann die Symbolleiste aus- und erneut eingeblendet werden.

Neue Schaltflächen können zu der Symbolleiste hinzugefügt und vorhandene Schaltflächen können aus ihr entfernt werden (s. Pkt. 5.6 auf S. 34).

Tabelle 3

Schalt-fläche	Menü	Funktion

Schalt-fläche	Menü	Funktion
	Service ⟶ Sicherheitsstufe	Auswahl der Sicherheitsstufe: • Alle blockieren • Hoch • Mittel • Niedrig • Alle erlauben Zu Details s. Pkt. 4.2 auf S. 21.
	Service ⟶ Regeln für Anwendungen	Öffnen des Konfigurationsfensters für die Anwendungsregeln.
	Service ⟶ Regeln für Paketfilterung	Öffnen des Konfigurationsfensters für die Paketfilterungsregeln.
	Ansicht ⟶Protokolle ⟶ Sicherheit	Öffnen des Fensters mit dem Sicherheitsprotokoll.
	Ansicht ⟶Anzeigen ⟶ Aktive Anwendungen	Öffnen einer Liste der gestarteten Netzwerk-Anwendungen.
	Ansicht ⟶Anzeigen ⟶ Offene Ports	Öffnen einer Liste der offenen Ports.
	Ansicht ⟶Anzeigen ⟶ Aktive Verbindungen	Öffnen einer Liste der aktiven Verbindungen.
	Service ⟶ Einstellungen	Öffnen des Konfigurationsfensters für Protokolleinstellungen, Einstellungen für die Aktivierung des Schutzes und Einstellungen des Angriffsdetektors.
	Hilfe ⟶ Inhalt	Öffnen des Hilfesystems

5.3.3. Arbeitsbereich

Im Arbeitsbereich des Programms befindet sich die *Skala der Sicherheitsstufen*, sowie Informationen über die aktuelle Sicherheitsstufe.

Die Skala der Sicherheitsstufen erlaubt die Auswahl unter fünf Stufen:

- Alle blockieren
- Hoch
- Mittel
- Niedrig
- Alle erlauben

Sie können die aktuelle Sicherheitsstufe ändern, indem Sie den Schieberegler auf der Skala bewegen. Danach erscheint rechts des Schiebereglers die Beschreibung der neuen Sicherheitsstufe (zu Details s. Pkt. 4.2 auf S. 21). Die Einstellungsänderungen werden sofort wirksam.

In den Sicherheitsstufen **Hoch**, **Mittel** und **Niedrig** können Sie mit Hilfe eines Kontrollkästchens die Zusatzfunktion **Stealth-Modus** aktivieren (s. Pkt. 4.2 auf S. 21).

Informationen über den aktuellen Systemstatus befinden sich im unteren Bereich des Arbeitsbereichs und enthalten Angaben über den zuletzt registrierten Hackerangriff: Datum, Uhrzeit und Typ des Angriffs sowie die Adresse des angreifenden Computers, wenn diese ermittelt werden konnte.

5.3.4. Statusleiste

Im unteren Bereich des Hauptfensters ist die *Statusleiste* angebracht. In ihr erscheint ein Kommentar für das im Moment gewählte Element des Hauptfensters. Sie können die Statusleiste durch die Auswahl des Punktes **Statusleiste** im Menü **Ansicht** ein- oder ausblenden.

5.4. Kontextmenü der Dialogfenster

Die Dialogfenster verfügen über ein *Kontextmenü*, das zur Ausführung von Operationen verwendet werden kann, die sich auf das jeweilige Fenster beziehen.

Das Kontextmenü eines Fensters wird durch Rechtsklick aufgerufen.

5.5. Assistent zur Regelerstellung

Der Assistent zur Regelerstellung besteht aus mehreren Dialogfenstern. Jedes Dialogfenster enthält eine bestimmte Auswahl von Schaltflächen zur Steuerung des Vorgangs der Regelerstellung. Wir erklären die Funktion der Schaltflächen:

- **Fertig stellen** – Erstellen der Regel
- **Abbrechen** – Verwerfen der Regelerstellung
- **Weiter** – einen Schritt weitergehen
- **Zurück** – einen Schritt zurückgehen.
- **Hilfe** – Aufruf des Hilfesystems

5.6. Ändern und Speichern von Eigenschaften der Benutzeroberfläche

*Um die Eigenschaften der Benutzeroberfläche zu ändern, wählen Sie im Menü **Ansicht** den Punkt **Symbolleisten**. Wählen Sie im folgenden Untermenü den Punkt **Anpassen**.*

Auf dem Bildschirm wird das Dialogfenster **Ändern** geöffnet (s. Abb. 6).

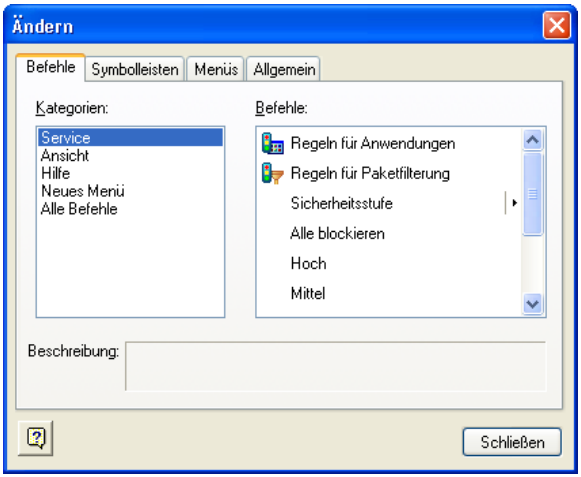


Abbildung 6. Dialogfenster **Ändern**

Zum Bearbeiten der Benutzeroberfläche empfehlen wir, das Fenster **Ändern** so zu platzieren, dass die Symbolleiste und das Hauptfenster des Programms gleichzeitig sichtbar sind.

Mit Hilfe der Registerkarte **Befehle** können Sie die Konfiguration des Hauptmenüs und der Symbolleiste vornehmen. Um einen neuen Befehl hinzuzufügen, wird mit der Maus der betreffende Befehl aus der Liste in das Menü oder auf die Symbolleiste verschoben. Zum Entfernen wird ein Befehl mit der Maus aus dem Hauptfenster heraus verschoben.

Auf den Registerkarten **Symbolleisten** und **Menü** können Sie das ursprüngliche Aussehen der Symbolleiste und des Menüs wiederherstellen.

Auf der Registerkarte **Allgemein** können Sie die Anzeige von QuickInfos zu den Schaltflächen der Symbolleiste aktivieren oder deaktivieren, die Größe der Schaltflächen festlegen sowie die Darstellungsreihenfolge der Menüpunkte konfigurieren.

Falls erwünscht, können Sie die Namen der Punkte des Hauptmenüs und der Schaltflächen ändern, Schaltflächen in Form von Text oder in Form eines Symbols darstellen.

Zum Ändern des Namens und/oder anderer Eigenschaften eines Hauptmenüpunktes oder einer Schaltfläche der Symbolleiste

1. Wählen Sie den gewünschten Punkt im Hauptmenü oder die gewünschte Schaltfläche auf der Symbolleiste, ohne das Fenster **Ändern** zu schließen.

2. Drücken Sie auf die rechte Maustaste. Wählen Sie im folgenden Kontextmenü die gewünschte Aktion:

   - **Löschen** – Entfernen des Punktes oder der Schaltfläche
   - **Schaltflächen-Erscheinungsbild** – Ändern des Namens. Ändern Sie im Feld **Schaltflächentext** des geöffneten gleichnamigen Dialogfensters den Namen des Punktes (s. Abb. 7). Klicken Sie auf die Schaltfläche **OK**.
   - **Nur Symbol** – nur das Symbol anzeigen
   - **Nur Text** – nur den Text anzeigen
   - **Symbol und Text** – Symbol und Text anzeigen
   - **Gruppe beginnen** – Teilungslinie einfügen

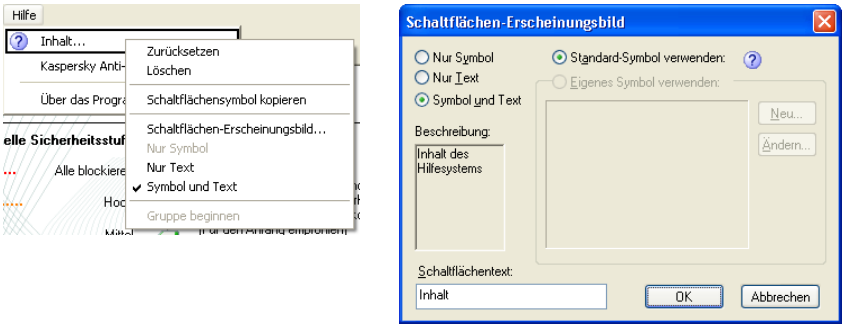


Abbildung 7. Ändern der Eigenschaften eines Befehls

Die Eigenschaften der Benutzeroberfläche werden automatisch gespeichert, treten sofort nach der Änderung in der aktuellen Sitzung in Kraft und gelten für alle folgenden Sitzungen.

5.7. Beenden des Programms

Um das Programm aus dem Arbeitsspeicher zu entfernen, wählen Sie im Kontextmenü des Programms oder im Menü **Service** des Programmhauptfensters den Punkt **Beenden**. Außerdem kann das Hauptfenster mit Hilfe der Schaltfläche in der oberen rechten Ecke des Programms geschlossen werden.

Das Schließen des Programmhauptfensters führt nicht zum Entfernen des Programms aus dem Arbeitsspeicher, wenn der Modus **Programm-Hauptfenster beim Schließen in den Infobereich der Taskleiste minimieren** aktiviert ist. In der Grundeinstellung ist dieser Modus aktiviert. Falls erwünscht, kann er deaktiviert werden (s. Pkt. 6.1.1 auf S. 38). Über die Präsenz des Programms im Arbeitsspeicher des Computers gibt das Programmsymbol in der Taskleiste Auskunft.

KAPITEL 6. AKTIVIERUNG UND EINSTELLUNGEN DES SCHUTZES

6.1. Aktivierung des Schutzes und Wahl der Sicherheitsstufe

6.1.1. Aktivierung des Schutzes

Der Schutz des Computers vor Hackerangriffen wird sofort nach dem Abschluss der Installation des Programms Kaspersky Anti-Hacker und dem Neustart des Computers aktiviert. Nach dem Programmstart erscheint im Infobereich der Taskleiste das Verknüpfungssymbol . In der Grundeinstellung arbeitet das Programm mit der Sicherheitsstufe **Mittel**. Beim Versuch einer Anwendung, eine Netzwerk-Operation auszuführen, wird der spezielle Konfigurationsmechanismus aufgerufen. Auf dem Bildschirm werden Informationen über die Anwendung, Parameter der Netzwerk-Operation und eine Abfrage für die Aktion (Erlauben oder Blockieren des aktuellen Ereignisses, Blockieren der Aktivität dieser Anwendung, Erlauben der Anwendungsaktivität in Übereinstimmung mit dem Typ, oder Konfiguration einer komplexen Regel für dieses Ereignis, die in Zukunft automatisch angewandt wird) angezeigt.

In der Standardeinstellung schützt Kaspersky Anti-Hacker den Computer nach der Anmeldung des Benutzers am System. Außerdem steht ein Modus zur Verfügung, in dem der Schutz sofort nach dem Start des Betriebssystems Windows in Aktion tritt.

Um den Start von Kaspersky Anti-Hacker sofort nach dem Laden des Betriebssystems zu deaktivieren/aktivieren:

1. Wählen Sie im Menü **Service** den Punkt **Einstellungen**.

2. Deaktivieren/aktivieren Sie im folgenden Dialogfenster **Einstellungen** (s. Abb. 8) auf der Registerkarte **Allgemein** das Kontrollkästchen

Programm bei Systemstart starten. Wenn Sie das Kontrollkästchen aktivieren, wird das Programm nach dem Laden des Betriebssystems mit den Benutzereinstellungen geladen. Da vor der Anmeldung des Benutzers am System die Anzeige des Konfigurationsfensters nicht möglich ist, werden bei Programmstart mit der Stufe **Mittel** alle unbekannten Netzwerk-Aktivitäten erlaubt. Ebenso erlaubt das Programm in den Sicherheitsstufen **Niedrig** und **Alle erlauben** unbekannte Netzwerk-Aktivität. In den übrigen Stufen wird diese blockiert.

Nehmen wir an, Ihr Computer ist mit einem lokalen Netzwerk verbunden, Sie haben die Aktivierung des Computerschutzes sofort nach dem Start des Betriebssystems festgelegt, und in den Einstellungen von Kaspersky Anti-Hacker die Sicherheitsstufe **Alle blockieren** gewählt oder in einer anderen Stufe (außer **Alle erlauben**) eine Regel für Paketfilterung erstellt, die jeden Netzwerk-Datenaustausch blockiert. In diesem Fall wird die Anmeldung am System länger dauern und nach der Anmeldung wird kein Zugriff auf das lokale Netzwerk bestehen.

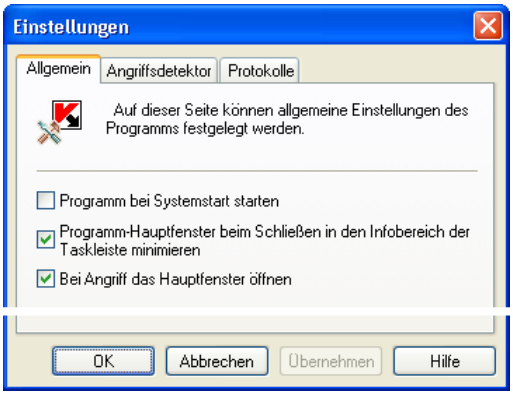


Abbildung 8. Dialogfenster **Einstellungen**

Die Reaktion des Programms für den Klick auf die Schaltfläche in der oberen rechten Ecke des Programms kann geändert werden. In der Grundeinstellung wird das Programmhauptfenster in diesem Fall geschlossen, aber das Programm wird nicht aus dem Arbeitsspeicher entfernt.

Um den Modus zu aktivieren, in dem beim Schließen des Programmhauptfensters das Programm aus dem Arbeitsspeicher entfernt wird,

1. Wählen Sie im Menü **Service** den Punkt **Einstellungen**.

2. Deaktivieren Sie im folgenden Dialogfenster **Einstellungen** (s. Abb. 8) auf der Registerkarte **Allgemein** das Kontrollkästchen **Programm-Hauptfenster beim Schließen in den Infobereich der Taskleiste minimieren**.

In der Grundeinstellung wird beim Entdecken eines Angriffs auf Ihren Computer das Hauptfenster mit einer Beschreibung des Angriffs auf dem Bildschirm geöffnet.

Damit das Hauptfenster nicht jedes Mal geöffnet wird, wenn ein Angriff entdeckt wird,

1. Wählen Sie im Menü **Service** den Punkt **Einstellungen**.

2. Deaktivieren Sie im folgenden Dialogfenster **Einstellungen** (s. Abb. 8) auf der Registerkarte **Allgemein** das Kontrollkästchen **Bei Angriff das Hauptfenster öffnen**.

6.1.2. Auswahl der Sicherheitsstufe

Die Auswahl der Sicherheitsstufe wird im Programmhauptfenster mit Hilfe des Schiebereglers der Skala für Sicherheitsstufen oder im Menü **Service** mit Hilfe des Punktes **Sicherheitsstufe** vorgenommen. Außerdem können Sie die Sicherheitsstufe mit Hilfe des gleichnamigen Punktes im Systemmenü ändern.

Sie können eine der folgenden fünf Schutzvarianten wählen:

- **Alle blockieren**
- **Hoch**
- **Mittel**
- **Niedrig**
- **Alle erlauben**

In den Sicherheitsstufen **Hoch**, **Mittel** und **Niedrig** können Sie die Zusatzfunktion mit Hilfe eines Kontrollkästchens **Stealth-Modus** aktivieren.

Die Modi werden sofort nach ihrer Auswahl wirksam.

Detaillierte Tipps zur Verwendung der Sicherheitsstufen finden Sie in Pkt. 4.2 auf S. 21.

6.1.3. Hinweis auf ein Netzwerk-Ereignis

Wenn Sie beim Erstellen einer Regel das Kontrollkästchen **Benutzer benachrichtigen** (s. Pkt. 6.3.2.3 auf S. 59, Pkt. 6.4.2.2 auf S. 68) aktiviert haben, dann wird bei Anwendung dieser Regel auf dem Bildschirm ein Hinweisfenster angezeigt (s. Abb. 9).

Auf Abb. 9 ist als Beispiel eine Benachrichtigung dargestellt, die bei Anwendung einer Regeln für Paketfilterung erscheint. Der Benachrichtigungstext enthält die Remote-Adresse, die lokale Adresse und die Verbindungsports.

Die angewandte Regel können Sie sich im entsprechenden Assistenten anzeigen lassen, wenn Sie auf den unterstrichenen Link klicken.

Außerdem können Sie die Anzeige solcher Hinweise in Zukunft abschalten, indem Sie das Kontrollkästchen **Diesen Hinweis nicht mehr anzeigen** aktivieren.

Kaspersky Anti-Hacker
Der Anwendung Internet Explorer wurde der Verbindungsaufbau mit Adresse 213.59.0.92 entsprechend der Regel
Remote-Port: 80
Lokaler Port: 1347 erlaubt
Diesen Hinweis nicht mehr anzeigen
OK

Abbildung 9. Benachrichtigung über ein Ereignis

Wenn Sie eine Regel erstellen, können Sie das Kontrollkästchen **Ereignis protokollieren** aktivieren, damit ein Eintrag über das betreffende Ereignis in das Protokoll aufgenommen wird.

6.1.4. Konfigurationsfenster

In der Sicherheitsstufe **Mittel** wird beim Eintreten eines Ereignisses, für das keine Reaktion in Form von Regeln festgelegt wurde, vom Programm das *Konfigurationsfenster* geöffnet (s. Abb. 10).

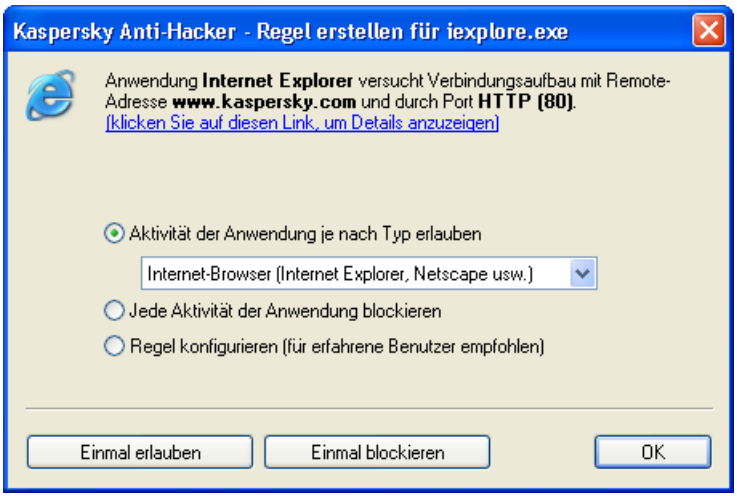

Kaspersky Anti-Hacker - Regel erstellen für iexplore.exe
Anwendung Internet Explorer versucht Verbindungsaufbau mit Remote-Adresse www.kaspersky.com und durch Port HTTP (80).
[klicken Sie auf diesen Link, um Details anzuzeigen]
Aktivität der Anwendung je nach Typ erlauben
Internet-Browser (Internet Explorer, Netscape usw.)
Jede Aktivität der Anwendung blockieren
Regel konfigurieren (für erfahrene Benutzer empfohlen)
Einmal erlauben
Einmal blockieren
OK

Abbildung 10. Dialogfenster **Regel erstellen für…**

Im oberen Bereich des Fensters sind folgende Elemente zu sehen: das Symbol und der Name der Anwendung, die versucht hat, eine Verbindung mit einem Remote-Computer aufzubauen, die Adresse dieses Computers und die Portnummer. Falls erwünscht, können Sie durch Klick auf den unterstrichenen Link detaillierte Informationen über die versuchte Verbindung erhalten.

Um eine konkrete Operation zu erlauben oder zu verbieten, wählen Sie die Schaltfläche **Einmal erlauben** oder **Einmal blockieren**.

Wenn Sie das Konfigurationsfenster durch Klick auf die Schaltfläche in der oberen rechten Ecke schließen, wird die betreffende Operation ein Mal blockiert.

Zum Erstellen einer Regel für die weitere Verarbeitung der Ereignisse, die durch diese Anwendung hervorgerufen wurden, wählen Sie eine der unten aufgezählten Aktionen und klicken Sie auf die Schaltfläche **OK**. Dadurch wird die neue Regel zu der Regelliste für Anwendungen hinzugefügt.

- **Aktivität dieser Anwendung je nach Typ erlauben** – Der Anwendung, die das Ereignis hervorgerufen hat, wird jede beliebige Netzwerk-Operation in Übereinstimmung mit dem Anwendungstyp erlaubt. Der Typ wird in der Dropdown-Liste festgelegt (zu Details s. Pkt. 6.3.2.1 auf S. 50).

- **Jede Aktivität dieser Anwendung blockieren** – Für die Anwendung, die das Ereignis hervorgerufen hat, werden sowohl die aktuelle Operation, als auch alle anderen Netzwerk-Operationen in Zukunft blockiert.

- **Regel konfigurieren** – Für die Anwendung werden die aktuelle Operation und andere Netzwerk-Operationen erlaubt oder verboten, wenn sie bestimmte Bedingungen erfüllen. Die Bedingungen werden nach Klick auf die Schaltfläche **OK** im Regelassistenten festgelegt (Einzelheiten über den Assistenten s. Pkt. 6.3.2 auf S. 49).

Sollte die von Ihnen erstellte Regel dem Programm die Reaktion auf das aktuelle Ereignis nicht erlauben, dann erscheint ein entsprechender Hinweis (s. Abb. 11). Klicken Sie zum Speichern der erstellten Regel auf die Schaltfläche **Ja**. Wenn Ihnen beim Erstellen der Regel ein Irrtum unterlaufen sein sollte, klicken Sie auf die Schaltfläche **Nein**. In beiden Fällen wird Ihnen die folgende Auswahl einer Aktion im Konfigurationsfenster vorgeschlagen.

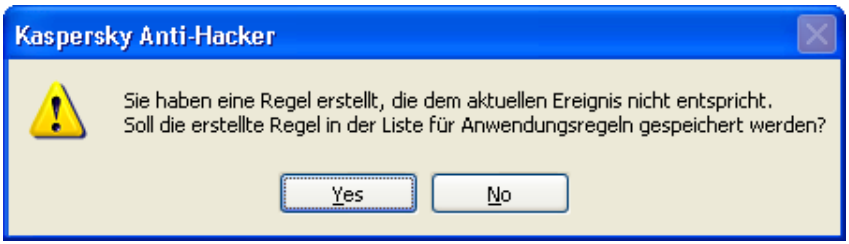

Kaspersky Anti-Hacker
Sie haben eine Regel erstellt, die dem aktuellen Ereignis nicht entspricht.
Soll die erstellte Regel in der Liste für Anwendungsregeln gespeichert werden?
Yes
No

Abbildung 11. Hinweis auf Widerspruch zwischen einer erstellten Regel und der Situation

Bitte beachten Sie Folgendes: Werden innerhalb einer kurzen Zeitspanne mehrere Programme gestartet, die versuchen, Netzwerk-Operationen auszuführen, für die noch keine Reaktion durch Regeln festgelegt wurde, dann wird eine *Warteschlange von Abfragen* auf das Erstellen neuer Regeln gebildet. Diese Abfragen werden nacheinander im Konfigurationsfenster angezeigt: Zuerst müssen Sie die Reaktion auf die Aktionen des ersten Netzwerk-Programms festlegen, danach auf jene des zweiten, usw. Alle Programme, die noch nicht an der Reihe waren, werden Ihre Reaktion abwarten.

6.1.5. Warnung über Veränderung eines ausführbaren Moduls

Kaspersky Anti-Hacker schützt Netzwerk-Anwendungen vor der Veränderung der ursprünglichen ausführbaren Dateien. Wird eine Veränderung festgestellt, dann gibt Kaspersky Anti-Hacker einen Warnhinweis aus (s. Abb. 12).

Daraufhin können Sie eine der folgenden Aktionen wählen:

- **Dieser Anwendung die weitere Netzwerk-Aktivität verbieten** – Für diese Anwendung werden alle folgenden Netzwerk-Operationen blockiert: Am Beginn der Liste wird eine Verbotsregel für diese Anwendung hinzugefügt und gleichzeitig werden alle früher für die Anwendung erstellten Regeln deaktiviert. Wir empfehlen Ihnen, die betreffende Anwendung mit einem Antiviren-Programm zu überprüfen, die Anwendung aus Ihrem Archiv wiederherzustellen oder sie neu zu installieren. Löschen sie nach der Wiederherstellung der Anwendung die betreffende Verbotsregel aus der Regelliste und reaktivieren Sie alle für diese erstellten Regeln. Sollte Kaspersky Anti-Hacker erneut eine Warnung über die Veränderung des ausführbaren Moduls anzeigen, dann wählen Sie die unten beschriebene Variante und fahren mit der Arbeit fort.

- **Mir ist bekannt, dass diese Datei verändert wurde und ich vertraue dieser Anwendung weiterhin** – Alle für die betreffende Anwendung gültigen Regeln gelten für die veränderte Datei weiter.

Klicken Sie auf die Schaltfläche **OK**.

Kaspersky Anti-Hacker - Veränderung iexplore.exe
Achtung! Die ausführbare Datei iexplore.exe wurde verändert. Bitte überprüfen Sie, ob Ihnen der Grund der Änderung bekannt ist (möglicherweise ein Versionsupdate) oder die Datei wurde infiziert. Untersuchen Sie diese Datei möglichst mit einem Antiviren-Programm.
Dieser Anwendung die weitere Netzwerk-Aktivität verbieten.
Mir ist bekannt, dass diese Datei verändert wurde und ich vertraue dieser Anwendung weiterhin.
OK

Abbildung 12. Warnung über die Veränderung einer ausführbaren Anwendungsdatei

6.2. Programmaktionen bei einem Angriff

Wird ein Hackerangriff entdeckt, dann wird aus der Systemleiste heraus das Programmhauptfenster eingeblendet (falls das Kontrollkästchen **Bei Angriff das Hauptfenster öffnen** aktiviert ist – s. Pkt. 6.1.1 auf S. 38). Bitte beachten Sie die Informationen über den erfolgten Hackerangriff im unteren Teil des Arbeitsbereichs: Dort gibt das Programm Datum, Uhrzeit und Typ des Angriffs an (s. Abb. 15).

Der Angriff wird abgewehrt. Außerdem wird der angreifende Computer für die in den Einstellungen festgelegte Zeit blockiert (s. Pkt. 6.5 auf S. 69).

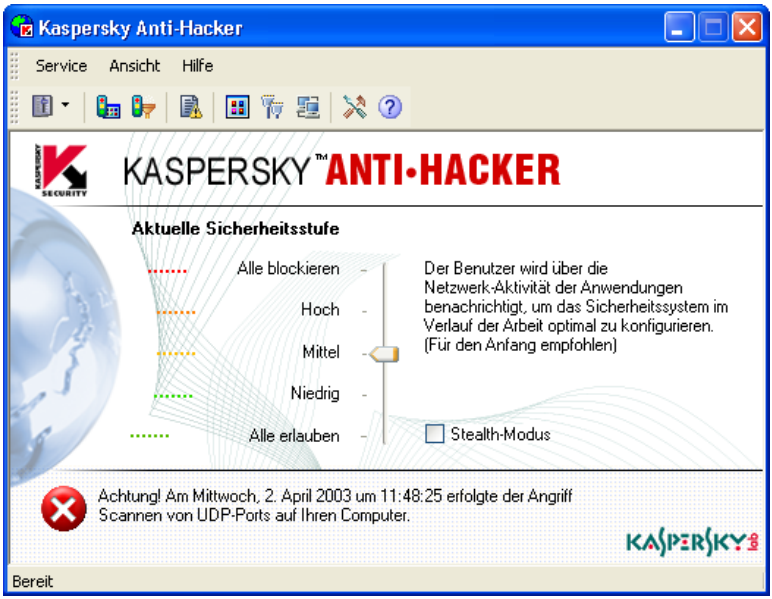


Abbildung 13. Meldung über die Entdeckung eines Hackerangriffs

Nehmen wir an, Sie haben bemerkt, dass von bestimmten Remote-Computern aus ständig Angriffe erfolgen. Dann können Sie den Datenaustausch Ihres Computers mit diesen Remote-Computern verbieten, indem Sie entsprechende Regeln für die Paketfilterung erstellen (s. Pkt. 6.4 auf S. 60).

Sollten sich Angriffe häufig wiederholen, dann empfehlen wir Ihnen, die Sicherheitsstufe **Alle blockieren** zu wählen und sich an Ihren Administrator oder Internet-Provider zu wenden.

6.3. Konfiguration der Regeln für Anwendungen

6.3.1. Arbeit mit der Regelliste

Um auf dem Bildschirm das Fenster zur Arbeit mit der Regelliste für Anwendungen zu öffnen,

wählen Sie im Programmmenü **Service** den Punkt **Regeln für Anwendungen**.

Danach wird auf dem Bildschirm das Dialogfenster **Regeln für Anwendungen** geöffnet (s. Abb. 14).

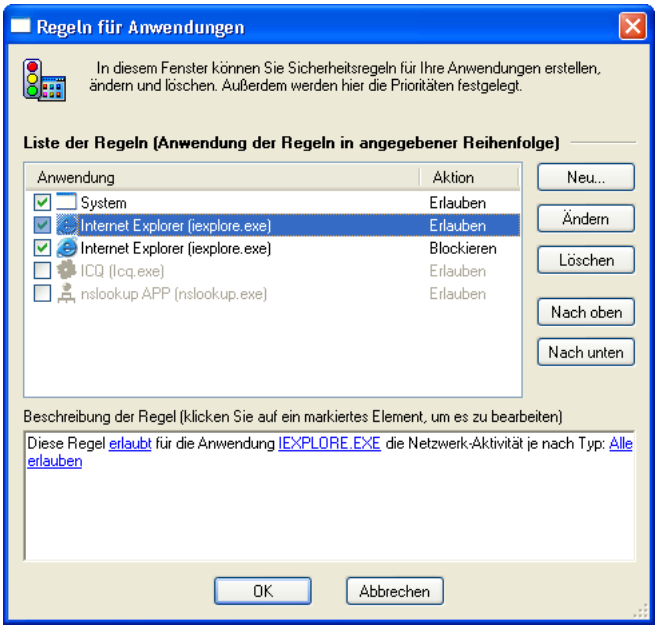


Abbildung 14. Dialogfenster **Regeln für Anwendungen**

Im linken Teil des Dialogfensters befindet sich die Regelliste für Anwendungen. In der Spalte "Anwendung" werden Symbol und Name der Anwendung, sowie ein Kontrollkästchen angezeigt, das angibt, ob diese Regel aktiviert oder deaktiviert ist. In der Spalte "Aktion" wird eine Kurzbeschreibung der Regel gegeben: **Erlauben** – für eine Erlaubnisregel, **Blockieren** – für eine Verbotsregel.

Die Regeln werden in der Reihenfolge ihrer Anwendungspriorität angezeigt: Die Regel, die an erster Stelle der Liste steht, wird zuerst angewandt, danach wird die zweite Regel der Liste angewandt, usw. Versucht eine Anwendung, eine Netzwerk-Operation auszuführen, dann wird die Regelliste von oben nach unten durchsucht, bis eine Regel gefunden wird, welche die betreffende Operation erlaubt oder verbietet, oder bis das Ende der Liste erreicht wird. Wird keine Regel gefunden, dann wird die Standard-Aktion angewandt (s. Pkt. 4.2 auf S. 21). Wenn Sie also für eine Anwendung nur bestimmte Operationen verbieten möchten, werden zwei Regeln erstellt – eine Regel, die in der Liste weiter oben steht und bestimmte Operationen erlaubt, und eine andere, die weiter unten steht und für diese Anwendung alle Operationen verbietet. Beim Versuch einer Anwendung, eine erlaubte Operation auszuführen, findet Kaspersky Anti-Hacker die Erlaubnisregel, beim Auftreten einer beliebigen anderen Operation hingegen die Verbotsregel.

So unterbindet in Abbildung 14 die dritte Regel beim MS Internet Explorer jede Netzaktivität, die zweite Regel erlaubt jedoch dem MS Internet Explorer den Zugriff auf das Internet mit dem HTTP-Protokoll. Da die zweite Regel höhere Priorität als die dritte Regel hat, kann der MS Internet Explorer eine Verbindung mit außen liegenden HTTP-Servern (und nur mit denen) aufbauen.

Bitte beachten Sie, dass nur Regeln angewandt werden, für die das entsprechende Kontrollkästchen links des Anwendungsnamens aktiviert ist. Auf Abb. 14 sind zum Beispiel die Regeln vier und fünf deaktiviert.

Zum vorübergehenden Aktivieren/Deaktivieren einer Regel der Liste der anzuwendenden Regeln

aktivieren/deaktivieren Sie das der Regel zugeordnete Kontrollkästchen in der Regelliste.

Rechts von der Regelliste befinden sich Steuerungsschaltflächen mit folgenden Funktionen:

- **Neu...** – Erstellen einer neuen Regel. Durch Klick auf diese Schaltfläche wird der Assistent zum Erstellen/Ändern von Regeln für Anwendungen aufgerufen.

- **Ändern** – Ändern einer aus der Liste gewählten Regel. Durch Klick auf diese Schaltfläche wird der Assistent aufgerufen, der Ihnen erlaubt, die Einstellungen der gewählten Regel zu ändern.

- **Entfernen** – Entfernen einer aus der Liste gewählten Regel

- **Nach oben** – Verschieben einer aus der Liste gewählten Regel um eine Zeile nach oben, d.h. Erhöhen ihrer Priorität

- **Nach unten** – Verschieben einer aus der Liste gewählten Regel um eine Zeile nach unten, d.h. Herabsetzen ihrer Priorität

Um eine aus der Liste gewählte Regel zu ändern, können Sie die **<EINGABE>**-Taste verwenden oder auf die Regel doppelklicken. Zum Entfernen einer aus der Liste gewählten Regel können Sie die Taste **<ENTF>** verwenden, um eine neue Regel hinzuzufügen die Taste <**EINFG>**.

Die Regelliste kann außerdem mit Hilfe des Kontextmenüs bearbeitet werden, das folgende Punkte enthält:

- **Ändern** – Ändern einer aus der Liste gewählten Regel

- **Entfernen** – Entfernen einer aus der Liste gewählten Regel

- **Regel kopieren** – Erstellen einer Kopie der aus der Liste gewählten Regel. Die erstellte Kopie wird unterhalb der gewählten Regel eingefügt.

Unter der Regelliste befindet sich ein Fenster mit einer Kurzbeschreibung der Regel, die in der Liste markiert ist. Ein solches Fenster finden Sie auch im Assistenten zum Erstellen und Ändern von Regeln. Wir behandeln es deshalb ausführlicher.

Im Fenster mit der Regelbeschreibung ist der unveränderbare Text der Regel schwarz geschrieben. Die Parameter der Regel, die verändert werden können, sind blau geschrieben und unterstrichen. Für durch fette Schrift hervorgehobene Parameter ist die Angabe eines Wertes obligatorisch.

Um den Wert eines Parameters für eine Regel anzugeben oder zu ändern,

1. Klicken Sie im Fenster mit der Regelbeschreibung auf den Parameter.

2. Wählen Sie im folgenden Dialogfenster den gewünschten Wert (die genaue Bedeutung der Parameter und die entsprechenden Dialogfenster werden in den folgenden Punkten erläutert).

Im unteren Teil des Dialogfensters **Regeln für Anwendungen** befinden sich folgende Schaltflächen:

- **OK** – Speichern der vorgenommenen Änderungen und Schließen des Fensters

- **Abbrechen** – Schließen des Fensters, ohne Speichern der Änderungen

Alle Änderungen der Regelliste werden sofort nach dem Speichern wirksam.

6.3.2. Hinzufügen einer neuen Regel

Um den Regelassistenten für Anwendungen aufzurufen,

klicken Sie im Dialogfenster **Regeln für Anwendungen** auf die Schaltfläche **Neu...** (s. Abb. 14).

6.3.2.1. Schritt 1. Konfiguration der Regel

Nach dem Aufruf des Assistenten erscheint das auf Abb. 15 dargestellte Fenster auf dem Bildschirm.

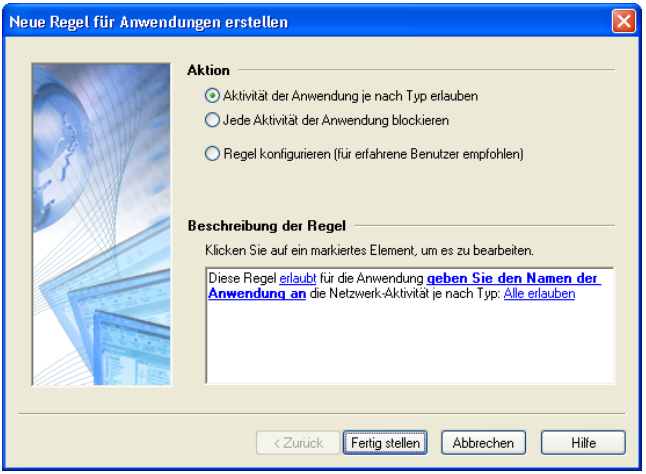

Neue Regel für Anwendungen erstellen
Aktion
Aktivität der Anwendung je nach Typ erlauben
Jede Aktivität der Anwendung blockieren
Regel konfigurieren (für erfahrene Benutzer empfohlen)
Beschreibung der Regel
Klicken Sie auf ein markiertes Element, um es zu bearbeiten.
Diese Regel erlaubt für die Anwendung geben Sie den Namen der Anwendung an die Netzwerk-Aktivität je nach Typ: Alle erlauben
< Zurück
Fertig stellen
Abbrechen
Hilfe

Abbildung 15. Das erste Fenster des Regelassistenten für Anwendungen

In der Liste **Aktion** können Sie zwischen drei Varianten wählen:

Aktion	Beschreibung der Regel
• **Aktivität dieser Anwendung je nach Typ erlauben**	Diese Regel erlaubt für die Anwendung IEXPLORE.EXE die Netzwerk-Aktivität je nach Typ: Internet-Browser (Internet Explorer, Netscape usw.)
• **Jede Aktivität dieser Anwendung blockieren**	Diese Regel blockiert für die Anwendung IEXPLORE.EXE jede Netzwerk-Aktivität
• **Regel konfigurieren**.	Diese Regel erlaubt für die Anwendung IEXPLORE.EXE den Verbindungsaufbau mit Remote-Computern nach Protokoll TCP

Bei Auswahl der Variante **Regel konfigurieren** können im nächsten Schritt des Assistenten die folgenden Zusatzparameter präzise eingestellt werden:

- Typ der Internet-Anwendung (Client oder Server)

- Protokoll
- Remote-Adresse
- Remote-Port
- Lokaler Port

Um eine Regel zu erstellen, die einer Anwendung Netzwerk-Operationen in Übereinstimmung mit dem Typ der Anwendung erlaubt,

1. Wählen Sie in der Liste **Aktion** die Option **Aktivität dieser Anwendung je nach Typ erlauben**.

2. Klicken Sie im Feld **Beschreibung der Regel** auf den Link Geben Sie den Namen der Anwendung an. Geben Sie im folgenden Fenster **Auswahl der Anwendung** den Namen der Anwendung an, auf die die Regel angewandt werden soll.

3. Der Anwendungstyp wird ebenfalls im Feld **Beschreibung der Regel** festgelegt. In der Grundeinstellung ist der Typ Alle erlauben angegeben, der die Aktionen einer Anwendung in keiner Weise einschränkt. Um den Typ zu ändern, klicken Sie auf diesen Link. Wählen Sie im folgenden Dialogfenster **Typ der Anwendung festlegen** (s. Abb. 16) in der Dropdown-Liste den gewünschten Wert und klicken Sie auf die Schaltfläche **OK**.

   - Internet-Browser – für Internet-Browser, Netscape Navigator und andere Webbrowser. Erlaubt wird die Arbeit nach den Protokollen HTTP, HTTPS, FTP und über Standard-Proxyserver.

   - Dateiübertragung – für Reget, Gozilla und ähnliche Programme. Erlaubt wird die Arbeit nach den Protokollen HTTP, HTTPS, FTP, TFTP und über Standard-Proxyserver.

   - E-Mail – für MS Outlook, MS Outlook Express, the Bat und andere
     E-Mail-Programme. Erlaubt wird die Arbeit nach den Protokollen SMTP, NNTP, POP3, IMAP4.

   - News – für Forte Agent und andere News-Programme. Erlaubt wird die Arbeit nach den Protokollen SMTP, NNTP.

- Instant-Messaging – für ICQ, AIM und andere Chat-Programme. Erlaubt wird die Arbeit über Standard-Proxyserver, sowie die Direktverbindung Ihres Computers mit dem Computer Ihres Gesprächspartners.

- Internet Rely Chat – für mIRC und ähnliche Programme. Erlaubt wird die Standard-Authentifizierung von Benutzern über IRC-Netzwerke und der Zugriff auf die Ports des IRC-Servers.

- Business-Konferenzen – für MS NetMeeting und ähnliche Programme. Erlaubt wird die Arbeit nach den Protokollen HTTP, HTTPS, über Standard-Proxyserver. Außerdem wird die Arbeit im lokalen Netzwerk (LDAP u.a.) unterstützt.

- Remote-Verwaltung – für Telnet u.ä. Erlaubt wird die Arbeit nach den Protokollen Telnet und SSH.

- Zeit-Synchronisation – für Timehook und ähnliche Programme. Erlaubt wird die Verbindung mit time- und daytime-Servern.

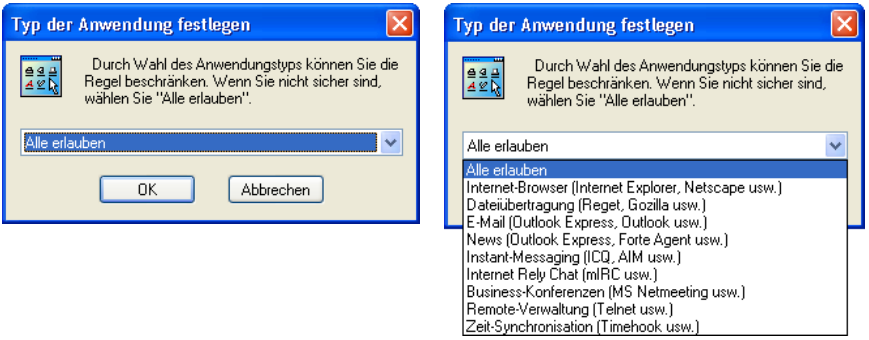

Typ der Anwendung festlegen
Durch Wahl des Anwendungstyps können Sie die Regel beschränken. Wenn Sie nicht sicher sind, wählen Sie "Alle erlauben".
Alle erlauben
OK
Abbrechen
Typ der Anwendung festlegen
Durch Wahl des Anwendungstyps können Sie die Regel beschränken. Wenn Sie nicht sicher sind, wählen Sie "Alle erlauben".
Alle erlauben
Alle erlauben
Internet-Browser (Internet Explorer, Netscape usw.)
Dateiübertragung (Reget, Gozilla usw.)
E-Mail (Outlook Express, Outlook usw.)
News (Outlook Express, Forte Agent usw.)
Instant-Messaging (ICQ, AIM usw.)
Internet Rely Chat (mIRC usw.)
Business-Konferenzen (MS Netmeeting usw.)
Remote-Verwaltung (Telnet usw.)
Zeit-Synchronisation (Timehook usw.)

Abbildung 16. Auswahl des Anwendungstyps

Um für eine Anwendung jede Netzwerk-Aktivität zu verbieten,

1. Wählen Sie in der Liste **Aktion** die Option **Jede Aktivität dieser Anwendung blockieren**.

2. Klicken Sie im Feld **Beschreibung der Regel** auf den Link Geben Sie den Namen der Anwendung an. Geben Sie im folgenden Fenster

Auswahl der Anwendung den Namen der Anwendung an, auf die die Verbotsregel angewandt werden soll.

Sollten die oben genannten Optionen für die Konfiguration von Regeln nicht ausreichend sein und Sie möchten zum Beispiel nur mit einer bestimmten IP-Adresse eine Verbindung aufbauen, dann geben Sie zusätzliche Regelparameter an.

Zur Konfiguration zusätzlicher Parameter einer Regel

1. Wählen Sie in der Liste **Aktion** die Option **Regel konfigurieren**.

2. Klicken Sie im Feld **Beschreibung der Regel** auf den Link Geben Sie den Namen der Anwendung an. Geben Sie im folgenden Fenster **Auswahl der Anwendung** den Namen der Anwendung an, auf die die Regel angewandt werden soll.

3. Klicken Sie im Feld **Beschreibung der Regel** auf den Link Erlaubt. Geben Sie im folgenden Fenster **Aktion festlegen** (s. Abb. 17) die gewünschte Aktion an und klicken Sie auf die Schaltfläche **OK**:

   - **Blockieren**

   - **Erlauben**.

4. Geben Sie an, auf welche Aktivität der Anwendung diese Regel reagieren soll: auf den Verbindungsaufbau (Standard) oder auf die Annahme eingehender Verbindungen. Um den vorgegebenen Wert zu ändern, klicken Sie im Feld **Beschreibung der Regel** auf den Link Verbindungsaufbau. Geben Sie im folgenden Dialogfenster **Aktivitätstyp der Anwendung wählen** (s. Abb. 18) die gewünschte Aktivitätsvariante **Annahme eingehender Netzwerk-Verbindungen von Remote-Computern** an und klicken Sie auf die Schaltfläche **OK**.

Klicken Sie nach der Angabe der Werte im ersten Fenster des Assistenten auf die Schaltfläche **Weiter**.

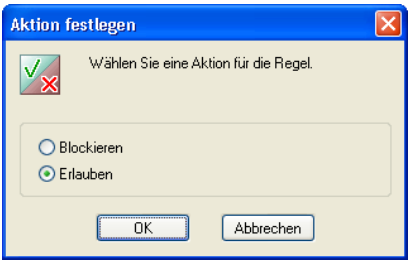


Abbildung 17. Aktion auswählen

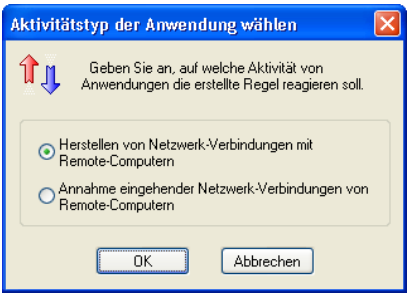

Aktivitätstyp der Anwendung wählen
Geben Sie an, auf welche Aktivität von Anwendungen die erstellte Regel reagieren soll.
Herstellen von Netzwerk-Verbindungen mit Remote-Computern
Annahme eingehender Netzwerk-Verbindungen von Remote-Computern
OK
Abbrechen

Abbildung 18. Aktivitätstyp der Anwendung wählen

Falls Sie auf die Schaltfläche **Weiter** klicken, ohne vorher eine Anwendung gewählt zu haben, erscheint ein Hinweis auf die erforderliche Eingabe im aktuellen Fenster des Assistenten.

6.3.2.2. Schritt 2. Bedingungen für die Anwendung der Regel

Das Fenster zur Angabe der Anwendungsbedingungen einer Regel erscheint nur, wenn Sie in der Liste **Aktion** die Option **Regel konfigurieren** gewählt haben.

In diesem Fenster können Sie das Protokoll, die Adresse des Remote-Computers und die Ports genau festlegen.

In der Dropdown-Liste **Protokoll** befindet sich eine Reihe verfügbarer Protokolle und ihnen entsprechende Portnummern:

- HTTP
- IMAP
- SMTP
- NNTP
- POP3
- DNS

Wenn Sie eine andere Portnummer festlegen möchten, wählen Sie den Wert:

- Anderes Protokoll auf TCP-Basis – für Dienste, die auf dem Protokoll TCP basieren

- Anderes Protokoll auf UDP-Basis – für Dienste, die auf dem Protokoll UDP basieren.

Im Feld **Parameter** befindet sich eine Liste mit Zusatzparametern, deren Elemente vom gewählten Protokoll abhängig sind.

Remote-Adresse – Adresse des Remote-Computers, mit dem ein Datenaustausch stattfinden soll. Zur Angabe der Adresse wird im Feld **Beschreibung der Regel** auf den Link Geben Sie die Adresse an geklickt. Wenn Sie eine Adressenliste anlegen möchten, halten Sie die Taste **<STRG>** gedrückt, während Sie auf den Link klicken. Zu Details s. Pkt. 6.3.2.2.1 auf S. 56.

Remote-Port – Nummer des Remote-Ports. Zur Angabe des Ports wird im Feld **Beschreibung der Regel** auf den Link Geben Sie den Port an geklickt, der sich rechts vom Link Remote-Port befindet. Wenn Sie eine Portliste anlegen möchten, halten Sie die Taste **<STRG>** gedrückt, während Sie auf den Link klicken. Zu Details s. Pkt. 6.3.2.2.2 auf S. 58.

Lokaler Port – Nummer des lokalen Ports. Zur Angabe des Ports wird im Feld **Beschreibung der Regel** auf den Link Geben Sie den Port an geklickt, der sich rechts vom Link Lokaler Port befindet. Wenn Sie eine Portliste anlegen möchten, halten Sie die Taste **<STRG>** gedrückt, während Sie auf den Link klicken. Zu Details s. Pkt. 6.3.2.2.2 auf S. 58.

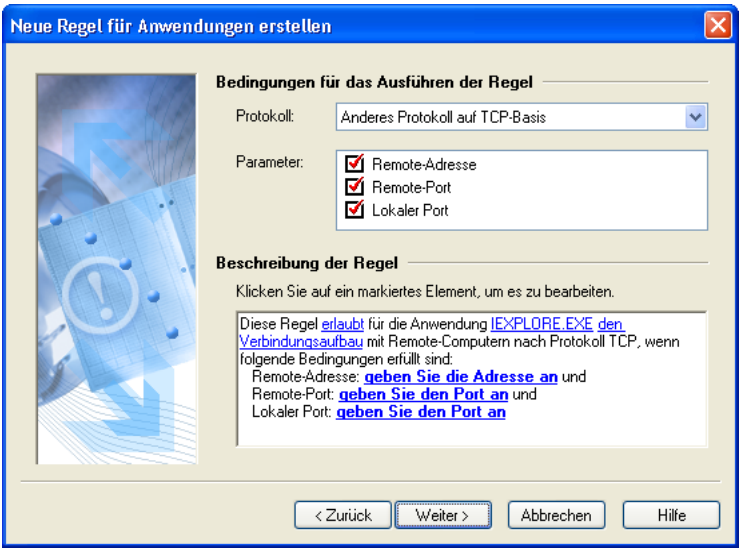

Neue Regel für Anwendungen erstellen
Bedingungen für das Ausführen der Regel
Protokoll:
Anderes Protokoll auf TCP-Basis
Parameter:
Remote-Adresse
Remote-Port
Lokaler Port
Beschreibung der Regel
Klicken Sie auf ein markiertes Element, um es zu bearbeiten.
Diese Regel erlaubt für die Anwendung IEXPLORE.EXE den Verbindungsaufbau mit Remote-Computern nach Protokoll TCP, wenn folgende Bedingungen erfüllt sind:
Remote-Adresse: geben Sie die Adresse an und
Remote-Port: geben Sie den Port an und
Lokaler Port: geben Sie den Port an
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 19. Angabe der Bedingungen für das Anwenden einer Regel

6.3.2.2.1. Angabe der Adresse oder des Adressbereichs

Die Angabe von Adressen wird mit Hilfe von zwei Dialogfenstern vorgenommen.

Das Dialogfenster **Adresse oder Adressbereich festlegen** (s. Abb. 20) erscheint, wenn Sie im Regelassistenten auf den Link zur Adressenangabe klicken, während Sie die Taste **<STRG>** gedrückt halten.

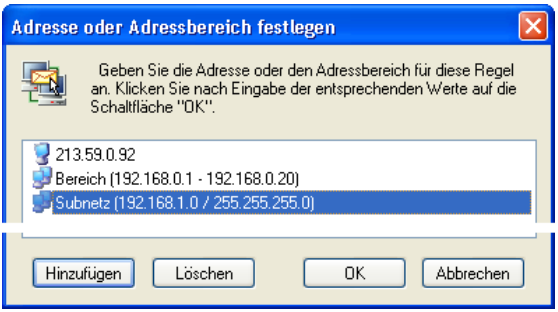

Adresse oder Adressbereich festlegen
Geben Sie die Adresse oder den Adressbereich für diese Regel an. Klicken Sie nach Eingabe der entsprechenden Werte auf die Schaltfläche "OK".
213.59.0.92
Bereich (192.168.0.1 - 192.168.0.20)
Subnetz (192.168.1.0 / 255.255.255.0)
Hinzufügen
Löschen
OK
Abbrechen

Abbildung 20. Dialogfenster **Adresse oder Adressbereich festlegen**

Zu der Liste, die sich in diesem Fenster befindet, können Sie mit Hilfe der Schaltflächen **Hinzufügen** und **Entfernen** beliebig viele Adressen, Adressbereiche und Subnetz-Adressen hinzufügen. Klicken Sie nach dem Erstellen der Adressenliste auf die Schaltfläche **OK**, um zum Regelassistenten zurückzukehren.

Durch Klick auf die Schaltfläche **Hinzufügen** im Fenster **Adresse oder Adressbereich festlegen** wird das Fenster **Adresse festlegen** geöffnet (s. Abb. 21). Dieses Fenster erscheint auch, wenn Sie direkt im Regelassistenten auf den Link zur Adressenangabe klicken.

Das Dialogfenster **Adresse festlegen** dient der Angabe einer Adresse, eines Adressbereichs oder einer Subnetz-Adresse, die in der Regel verwendet werden sollen (s. Abb. 21).

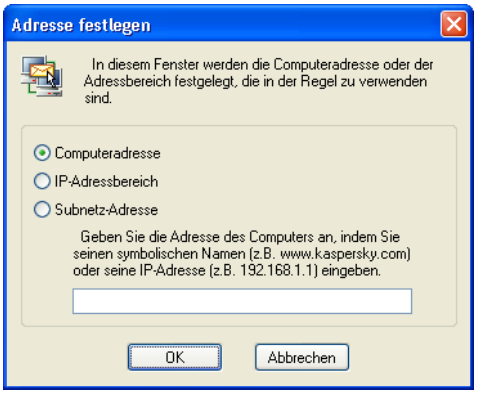

Adresse festlegen
In diesem Fenster werden die Computeradresse oder der Adressbereich festgelegt, die in der Regel zu verwenden sind.
Computeradresse
IP-Adressbereich
Subnetz-Adresse
Geben Sie die Adresse des Computers an, indem Sie seinen symbolischen Namen (z.B. www.kaspersky.com) oder seine IP-Adresse (z.B. 192.168.1.1) eingeben.
OK
Abbrechen

Abbildung 21. Dialogfenster **Adresse festlegen**. Angabe der Computeradresse

Sie können zwischen drei Varianten wählen:

- **Computeradresse** – Im Eingabefeld wird der symbolische Name des Computers (zum Beispiel: `www.kaspersky.com`) oder dessen IP-Adresse (zum Beispiel: `192.68.1.1`) angegeben.

- **IP-Adressbereich** – Im Eingabefeld **Untere Grenze** wird die erste IP-Adresse des Adressbereichs und im Feld **Obere Grenze** die letzte IP-Adresse des Bereichs angegeben (s. Abb. 22).

- **Subnetz-Adresse** – Im Eingabefeld **Subnetz-Adresse** wird die Adresse des Subnetzes und im Feld **Subnetz-Maske** dessen Maske angegeben (s. Abb. 23).

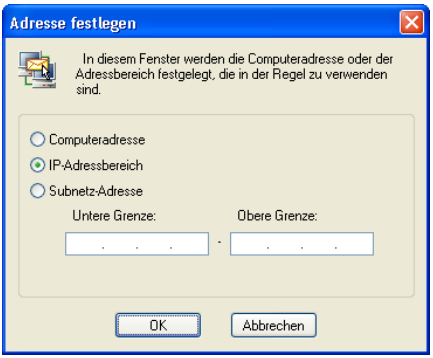


Abbildung 22. Angabe des Adressbereichs

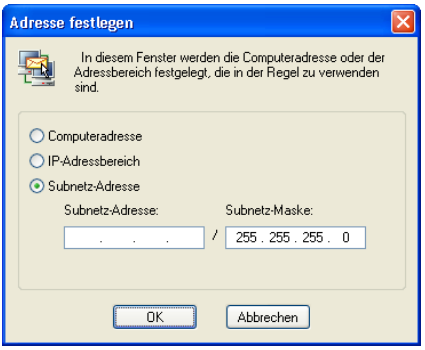


Abbildung 23. Angabe des Subnetzes

Klicken Sie nach der Angabe der Adresse auf die Schaltfläche **OK**.

6.3.2.2.2. Angabe des Ports

Die Angabe der Portnummern wird mit Hilfe von zwei Dialogfenstern vorgenommen.

Das Dialogfenster **Port oder Portbereich festlegen** (s. Abb. 24) wird geöffnet, wenn Sie im Regelassistenten auf die Zeile mit dem Namen des Portparameters klicken, während Sie die Taste **<STRG>** gedrückt halten.

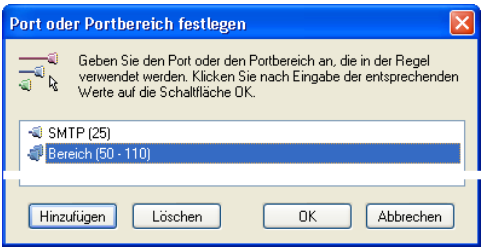

Port oder Portbereich festlegen
Geben Sie den Port oder den Portbereich an, die in der Regel verwendet werden. Klicken Sie nach Eingabe der entsprechenden Werte auf die Schaltfläche OK.
SMTP (25)
Bereich (50 - 110)
Hinzufügen
Löschen
OK
Abbrechen

Abbildung 24. Dialogfenster **Port oder Portbereich festlegen**

Zu der Liste, die sich in diesem Fenster befindet, können Sie mit Hilfe der Schaltflächen **Hinzufügen** und **Entfernen** eine beliebige Anzahl von Ports und Portnummernbereichen hinzufügen. Klicken Sie nach dem Erstellen der Portliste auf die Schaltfläche **OK**, um zum Regelassistenten zurückzukehren.

Durch Klick auf die Schaltfläche **Hinzufügen** im Fenster **Port oder Portbereich festlegen** wird das Fenster **Port** geöffnet (s. Abb. 25). Dieses Fenster erscheint auch, wenn Sie direkt im Regelassistenten auf die Zeile mit dem Namen des Portparameters klicken.

Das Dialogfenster **Port** dient der Angabe einer Portnummer oder eines Portnummernbereichs, die in der Regel verwendet werden sollen (s. Abb. 25).

Zwei Varianten stehen zur Auswahl:

- **Portnummer festlegen** – Im Eingabefeld der Dropdown-Liste können Sie einen der vorhandenen Werte wählen oder manuell eine Portnummer angeben.

- **Portbereich festlegen** – Im ersten Feld wird Anfangsnummer des Portbereichs und im zweiten Feld die Endnummer des Bereichs angegeben (s. Abb. 26).

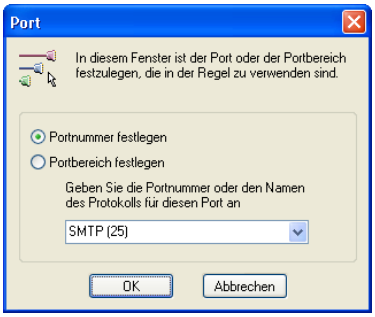

Port
In diesem Fenster ist der Port oder der Portbereich festzulegen, die in der Regel zu verwenden sind.
Portnummer festlegen
Portbereich festlegen
Geben Sie die Portnummer oder den Namen des Protokolls für diesen Port an
SMTP (25)
OK
Abbrechen

Abbildung 25. Dialogfenster **Port**

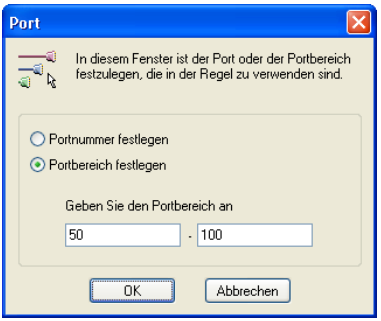


Abbildung 26. Angabe eines Portbereichs

Klicken Sie nach der Angabe der Portnummern auf die Schaltfläche **OK**.

6.3.2.3. Schritt 3. Angabe der zusätzlichen Aktionen

Als zusätzliche Aktionen können Sie das Kontrollkästchen **Ereignis protokollieren** aktivieren, damit ein Eintrag über das betreffende Ereignis in das Protokoll aufgenommen wird. Außerdem können Sie das Kontrollkästchen

Benutzer benachrichtigen aktivieren, damit beim Eintreten des Ereignisses eine Warnung auf dem Bildschirm erscheint (s. Abb. 9).

Neue Regel für Anwendungen erstellen
Zusätzliche Aktion
Ereignis protokollieren
Benutzer benachrichtigen
Beschreibung der Regel
Klicken Sie auf ein markiertes Element, um es zu bearbeiten.
Diese Regel erlaubt für die Anwendung IEXPLORE.EXE die Annahme eingehender Verbindungen von Remote-Computern nach Protokoll TCP
Bei Anwendung der Regel wird das Ereignis protokolliert und wird der Benutzer benachrichtigt
< Zurück
Fertig stellen
Abbrechen
Hilfe

Abbildung 27. Zusätzliche Aktionen

6.4. Konfiguration der Regeln für Paketfilterung

6.4.1. Arbeit mit der Regelliste

Die Arbeit mit den Regeln für Paketfilterung entspricht der Arbeit mit den Regeln für Anwendungen.

Um auf dem Bildschirm das Fenster zur Arbeit mit der Regelliste für Paketfilterung öffnen,

wählen Sie im Programmmenü **Service** den Punkt **Regeln für Paketfilterung**.

Dadurch wird auf dem Bildschirm das Dialogfenster **Regeln für Paketfilterung** geöffnet (s. Abb. 28).

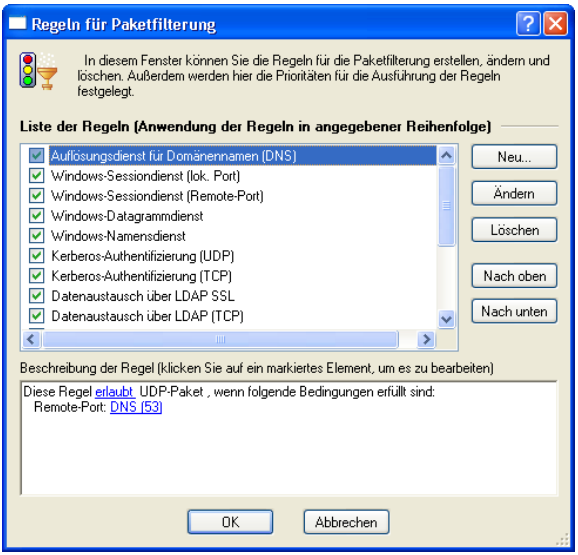

Regeln für Paketfilterung
In diesem Fenster können Sie die Regeln für die Paketfilterung erstellen, ändern und löschen. Außerdem werden hier die Prioritäten für die Ausführung der Regeln festgelegt.
Liste der Regeln (Anwendung der Regeln in angegebener Reihenfolge)
Auflösungsdienst für Domänennamen (DNS)
Windows-Sessiondienst (lok. Port)
Windows-Sessiondienst (Remote-Port)
Windows-Datagrammdienst
Windows-Namensdienst
Kerberos-Authentifizierung (UDP)
Kerberos-Authentifizierung (TCP)
Datenaustausch über LDAP SSL
Datenaustausch über LDAP (TCP)
Neu...
Ändern
Löschen
Nach oben
Nach unten
Beschreibung der Regel (klicken Sie auf ein markiertes Element, um es zu bearbeiten)
Diese Regel erlaubt UDP-Paket , wenn folgende Bedingungen erfüllt sind:
Remote-Port: DNS (53)
OK
Abbrechen

Abbildung 28. Dialogfenster **Regeln für Paketfilterung**

Im linken Teil des Dialogfensters befindet sich die Regelliste für die Paketfilterung. In jeder Zeile ist vor dem Namen der Regel ein Kontrollkästchen angebracht, das zeigt, ob die Regel aktiviert oder deaktiviert ist.

Die Regeln werden in der Reihenfolge ihrer Anwendungspriorität angezeigt: Die Regel, die an erster Stelle der Liste steht, wird zuerst angewandt, danach wird die zweite Regel der Liste angewandt, usw. Bitte beachten Sie, dass nur Regeln angewandt werden, für die das entsprechende Kontrollkästchen links von ihrem Namen aktiviert ist.

Zum vorübergehenden Aktivieren/Deaktivieren einer Regel der Liste der anzuwendenden Regeln

aktivieren/deaktivieren Sie das der Regel zugeordnete Kontrollkästchen in der Regelliste.

Rechts von der Regelliste befinden sich Steuerungsschaltflächen mit folgenden Funktionen:

- **Neu...** – Erstellen einer neuen Regel. Durch Klick auf diese Schaltfläche wird der Assistent zum Erstellen einer neuen Paketfilterungsregel aufgerufen.

- **Ändern** – Ändern einer aus der Liste gewählten Regel. Durch Klick auf diese Schaltfläche wird der Assistent zum Ändern einer Regel für Paketfilterung aufgerufen.

- **Entfernen** – Entfernen einer aus der Liste gewählten Regel

- **Nach oben** – Verschieben einer aus der Liste gewählten Regel um eine Zeile nach oben, d.h. Erhöhen ihrer Priorität

- **Nach unten** – Verschieben einer aus der Liste gewählten Regel um eine Zeile nach unten, d.h. Herabsetzen ihrer Priorität

Um eine aus der Liste gewählte Regel zu ändern, können Sie die **<EINGABE>**-Taste verwenden oder auf die Regel doppelklicken. Zum Entfernen einer aus der Liste gewählten Regel können Sie die Taste **<ENTF>** verwenden, um eine neue Regel hinzuzufügen die Taste **<EINFG>**.

Die Regelliste kann außerdem mit Hilfe des Kontextmenüs bearbeitet werden, das folgende Punkte enthält:

- **Ändern** – Ändern einer aus der Liste gewählten Regel

- **Entfernen** – Entfernen einer aus der Liste gewählten Regel

- **Regel kopieren** – Erstellen einer Kopie der aus der Liste gewählten Regel. Die erstellte Kopie wird unterhalb der gewählten Regel eingefügt.

Unter der Regelliste befindet sich ein Fenster mit einer Kurzbeschreibung der Regel, die in der Liste markiert ist. Ein solches Fenster finden Sie auch im Assistenten zum Erstellen und Ändern von Regeln. Wir behandeln es deshalb ausführlicher.

Im Fenster mit der Regelbeschreibung ist der unveränderbare Text der Regel schwarz geschrieben. Die Parameter der Regel, die verändert werden können, sind blau geschrieben und unterstrichen. Für durch fette Schrift hervorgehobene Parameter ist die Angabe eines Wertes obligatorisch.

Um den Wert eines Parameters für eine Regel anzugeben oder zu ändern,

1. Klicken Sie im Fenster mit der Regelbeschreibung auf den Parameter.
2. Wählen Sie im folgenden Dialogfenster den gewünschten Wert (die genaue Bedeutung der Parameter und die entsprechenden Dialogfenster werden in den folgenden Punkten erläutert).

Im unteren Teil des Dialogfensters **Regeln für Paketfilterung** befinden sich folgende Schaltflächen:

- **OK** – Speichern der vorgenommenen Änderungen und Schließen des Fensters
- **Abbrechen** – Schließen des Fensters, ohne Speichern der Änderungen

Alle Änderungen der Regelliste werden sofort nach dem Speichern wirksam.

Die Regeln für Paketfilterung verfügen über eine höhere Priorität als die Regeln für Anwendungen und werden folglich zuerst angewandt.

6.4.2. Hinzufügen einer neuen Regel

Der Assistent zum Hinzufügen von Paketfilterungsregeln entspricht dem Assistenten zum Hinzufügen von Anwendungsregeln und besteht aus zwei Schritten.

6.4.2.1. Schritt 1. Angabe der Bedingungen für die Anwendung der Regel

Im ersten Schritt der Regeldefinition für Paketfilterung können Sie folgende Parameter festlegen:

- verwendetes Protokoll (TCP, UDP, ICMP, Andere IP-Protokolle)
- Zieladresse der Pakete
- Richtung der Paketübertragung (eingehend, ausgehend)
- spezifische Werte für die einzelnen Protokolle (für TCP- und UDP-Protokolle – Ports, für ICMP-Protokolle – Meldungstypen, für andere IP-Protokolle – Protokollnummer)
- Aktion (erlauben/blockieren)

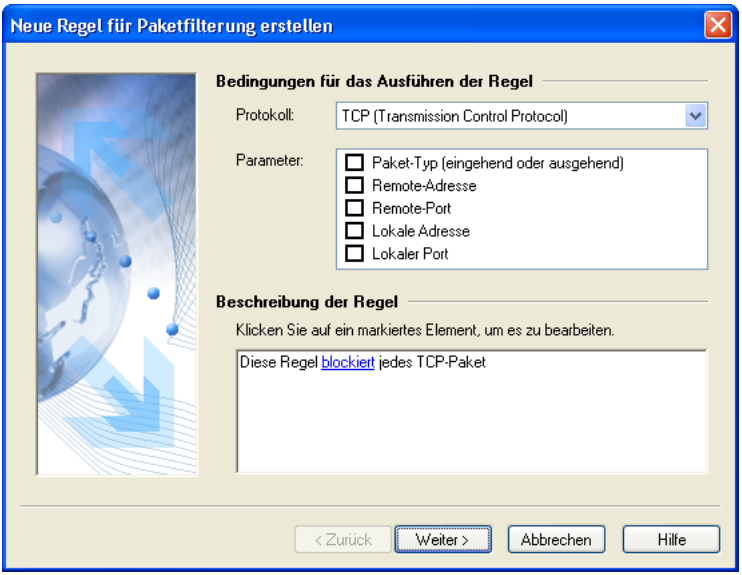


Abbildung 29. Das erste Fenster des Regelassistenten für Paketfilterung

Um eine Filterregel zu erstellen,

1. Wählen Sie das zu filternde Protokoll in der Dropdown-Liste Protokoll: Mögliche Protokollvarianten: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), Andere IP-Protokolle. Als Standard wird der Punkt TCP angezeigt.

2. Aktivieren Sie im Feld Parameter die gewünschten Kontrollkästchen:

Paket-Typ (eingehend oder ausgehend) – Richtung der Paketübertragung. In der Grundeinstellung ist das Kontrollkästchen deaktiviert, was der Kontrolle der Datenübertragung in beiden Richtungen entspricht. Wenn Sie möchten, dass das Programm nur eingehende oder nur ausgehende Pakete kontrolliert, dann aktivieren Sie das Kontrollkästchen und legen Sie die Richtung der Datenübertragung im Feld **Beschreibung der Regel** fest. Zur Angabe der Datenübertragungsrichtung wird auf den Link mit der Richtungsangabe geklickt. Wählen Sie im folgenden Dialogfenster

Richtung der Paketübertragung festlegen die gewünschte Variante und klicken Sie auf die Schaltfläche **OK**.

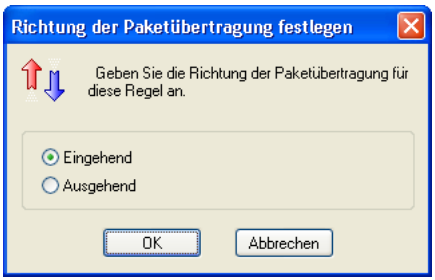


Abbildung 30. Dialogfenster **Richtung der Paketübertragung festlegen**

3. Im Feld **Parameter** befindet sich außerdem eine Liste zusätzlicher Parameter, deren Auswahl vom gewählten Protokoll abhängig ist:

   - Für ein TCP- und UDP-Protokoll können **Remote-Port** und **Lokaler Port** festgelegt werden.
   - Für ein ICMP-Protokoll kann der **Typ der ICMP-Meldung** festgelegt werden.
   - Für andere Protokolle auf IP-Basis kann das **Protokoll** festgelegt werden.

☑ **Remote-Adresse** – Adresse des Remote-Computers (für alle Protokolle).

☑ **Lokale Adresse** – Adresse des lokalen Computers (für alle Protokolle).

Zur Angabe der Adresse wird im Feld **Beschreibung der Regel** auf den Link "geben Sie die Adresse an" geklickt, der sich rechts der Zeile "Remote-Adresse" bzw. "Lokale Adresse" befindet. Wenn Sie eine Adressenliste anlegen möchten, halten Sie die Taste **<STRG>** gedrückt, während Sie auf den Link klicken. Zu Details s. Pkt. 6.3.2.2.1 auf S. 56.

☑ **Remote-Port** – Nummer des Ports auf dem Remote-Computer (für TCP- und UDP-Protokolle).

☑ **Lokaler Port** – Nummer des Ports auf dem lokalen Computer (für TCP- und UDP-Protokolle).

Zur Angabe des Ports wird im Feld **Beschreibung der Regel** auf den Link "Port festlegen" geklickt, der sich rechts von der Zeile "Remote-Port" bzw. "Lokaler Port" befindet. Zu Details s. Pkt. 6.3.2.2.2 auf S. 58. Wenn Sie eine Portliste anlegen möchten, halten Sie die Taste **<STRG>** gedrückt, während Sie auf den Link klicken. Zu Details s. Pkt. 6.3.2.2.1 auf S. 56.

Typ der ICMP-Meldung – Typ der ICMP-Meldung (nur für ICMP-Protokoll). Zur Angabe des Typs wird im Feld **Beschreibung der Regel** auf den Link "geben Sie den Typ der Meldung an" geklickt. Wählen Sie im folgenden Dialogfenster **Typ der ICMP-Meldungen festlegen** (s. Abb. 31) den gewünschten Wert und klicken Sie auf die Schaltfläche **OK**.

- Echoanforderung
- Echoantwort
- Zeitüberschreitung (TTL exceed)
- Netzwerk nicht erreichbar
- Host nicht erreichbar
- Protokoll nicht erreichbar
- Port nicht erreichbar
- Umleitung für Host
- Umleitung für Netzwerk
- Umleitung für TOS und Netzwerk
- Umleitung für TOS und Host

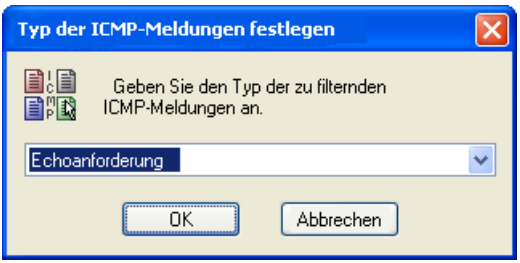


Abbildung 31. Dialogfenster **Typ der ICMP-Meldungen festlegen**

Protokoll – Name oder Nummer des Protokolls (nur für IP-Protokolle). Wenn Sie dieses Kontrollkästchen nicht aktivieren, werden alle IP-Protokolle gefiltert. Zur Angabe eines bestimmten Protokolls aktivieren Sie das Kontrollkästchen und klicken Sie im Feld **Beschreibung der Regel** auf den Link "geben Sie das Protokoll an". Wählen Sie in der Dropdown-Liste des

Dialogfensters **Protokoll festlegen** (s. Abb. 32) den gewünschten Wert und klicken Sie auf die Schaltfläche **OK**. In der unten folgenden Protokoll-Liste wird in Klammern die entsprechende Nummer des Protokolls angegeben.

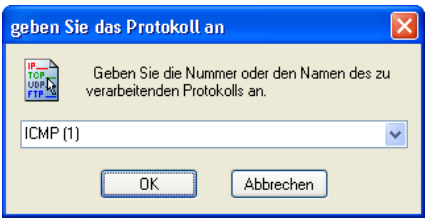


Abbildung 32. Dialogfenster **Protokoll**

- ICMP(1)
- IGMP,RGMP(2)
- GGP(3)
- IP in IP (Verkapselung) (4)
- TCP(6)
- IGRP(9)
- UDP(17)
- GRE(47)
- ESP(50)
- AH(51)
- IP mit Verschlüsselung(53).

4. Legen Sie die Aktion fest, die das Programm beim Entdecken eines Pakets ausführen soll, das die oben genannten Bedingungen erfüllt: Blockieren oder Erlauben. In der Grundeinstellung werden solche Pakete blockiert. Um diesen Wert zu ändern, klicken Sie im Feld **Beschreibung der Regel** auf den entsprechenden Link. Wählen Sie im folgenden Fenster **Aktion festlegen** die gewünschte Aktion und klicken Sie auf die Schaltfläche **OK** (s. Abb. 33).

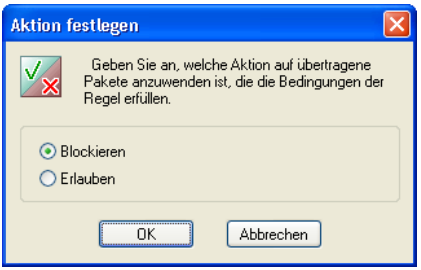


Abbildung 33. Dialogfenster **Aktion festlegen**

6.4.2.2. Schritt 2. Angabe eines Namens für die Regel und zusätzlicher Aktionen

Im zweiten Schritt zum Erstellen einer Paketfilterungsregel ist die Angabe eines Namens für die Regel im Feld **Name der Regel** erforderlich. Der Name der Regel wird in die Regelliste aufgenommen und hilft beim Auffinden der Regeln. Als Standard wird ein einheitlicher Regelname der folgenden Form vorgeschlagen: "Regel für Paketfilterung #<Nummer der Regel>". Wir empfehlen Ihnen die Vergabe von aussagefähigen Namen, die der Spezifik der Regeln entsprechen.

Es stehen zwei zusätzliche Aktionen zur Verfügung: Sie können das Kontrollkästchen **Ereignis protokollieren** aktivieren, damit ein Eintrag über das betreffende Ereignis in das Protokoll aufgenommen wird. Außerdem können Sie das Kontrollkästchen **Benutzer benachrichtigen** aktivieren, damit beim Eintreten des Ereignisses eine Warnung auf dem Bildschirm erscheint (s. Abb. 9).

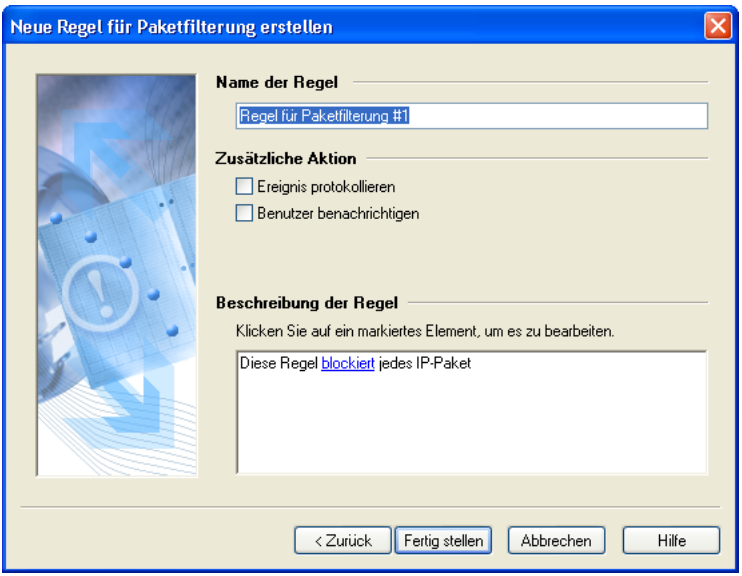


Abbildung 34. Angabe des Regelnamens und der zusätzlichen Aktionen

6.5. Angriffsdetektor

6.5.1. Konfigurationsfenster des Angriffsdetektors

Zum Öffnen des Fensters mit den Einstellungen des Angriffsdetektors

wählen Sie im Menü **Service** den Punkt **Einstellungen** und gehen Sie auf die Registerkarte **Angriffsdetektor** (s. Abb. 35).

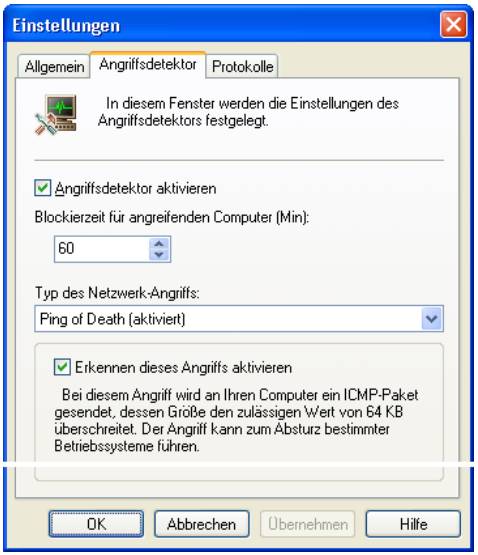


Abbildung 35. Registerkarte **Angriffsdetektor** des Dialogfensters **Einstellungen**

Wir empfehlen Ihnen, das Kontrollkästchen **Angriffsdetektor aktivieren**, das sich im oberen Teil der Registerkarte befindet, nie zu deaktivieren. Dieses Kontrollkästchen dient der Aktivierung und Deaktivierung des Angriffsdetektors auf Ihrem Computer.

Darunter ist das Zahlenfeld **Blockierzeit für angreifenden Computer** angebracht, das angibt, für wie viele Minuten ein angreifender Computer

vollständig blockiert wird, falls seine Adresse ermittelt werden kann. Dieser Parameter gilt generell für alle Angriffstypen.

Eine Änderung des Wertes für die **Blockierzeit für angreifenden Computer** wird sofort nach dem Klick auf die Schaltfläche **OK** oder **Übernehmen** im Fenster **Einstellungen** wirksam und gilt für alle danach erkannten Angriffe. Für Computer, die auf Grund bereits erfolgter Angriffe blockiert sind, ändert sich die Blockierzeit nicht.

Die Auswahl der unteren Teil des Fensters angebrachten Felder ändert sich in Abhängigkeit des Angriffstyps, der in der Dropdown-Liste **Typ des Netzwerk-Angriffs** gewählt wird.

Aktivieren Sie das Kontrollkästchen **Erkennen dieses Angriffs aktivieren**, wenn Sie möchten, dass Angriffe des entsprechenden Typs erkannt werden. Bei der Entscheidung kann Ihnen die Beschreibung des Angriffs behilflich sein, die unterhalb des Kontrollkästchens gegeben wird.

6.5.2. Liste der feststellbaren Hackerangriffe

Kaspersky Anti-Hacker erkennt die verbreiteten DoS-Angriffe (*SYN Flood, UDP Flood, ICMP Flood*), die Angriffe *Ping of death, Land, Helkern, SmbDie, und Lovesan*, und verfolgt das Scannen von Ports, das gewöhnlich gefährlicheren Angriffen vorausgeht:

- ***Ping of Death***: Bei diesem Angriff wird ein ICMP-Paket gesendet, dessen Größe den zulässigen Wert von 64 KB überschreitet. Der Angriff kann zum Absturz bestimmter Betriebssysteme führen.

- ***Land***: Bei diesem Angriff wird an einen offenen Port des angegriffenen Computers eine Anfrage auf Verbindungsherstellung mit sich selbst gesendet. Dies führt zu einer Endlosschleife im angegriffenen Computer, was eine stark erhöhte Prozessorbelastung zur Folge hat und zum Absturz des Betriebssystems führen kann.

- ***Scannen von TCP-Ports***: Dabei werden die offenen TCP-Ports auf einem angegriffenen Computer ermittelt. Der Angriff dient der Suche nach Schwachstellen im Computersystem und geht meist gefährlicheren Angriffen voraus. Für diesen Angriff können Sie durch **Anzahl der Ports** die Anzahl der Ports festlegen, die ein Remote-Computer innerhalb des durch **Zeit (Sek)** angegebenen Zeitraums zu öffnen versucht.

- ***Scannen von UDP-Ports**:* Dabei werden analog zum Scannen von TCP-Ports die offenen UDP-Ports auf einem angegriffenen Computer ermittelt. Dieser Angriff kann durch die Kontrolle der Anzahl von UDP-Paketen erkannt werden, die auf bestimmten Ports des angegriffenen Computers innerhalb eines bestimmten Zeitraums gesendet werden. Der Angriff dient der Suche nach Schwachstellen im Computersystem und geht meist gefährlicheren Angriffen voraus. Für diesen Angriff können Sie durch **Anzahl der Ports** die Anzahl der Ports festlegen, die ein Remote-Computer innerhalb des durch **Zeit (Sek)** angegebenen Zeitraums zu öffnen versucht.

- ***SYN Flood**:* Bei diesem Angriff werden große Mengen falscher Verbindungsanfragen an den angegriffenen Computer gesendet. Das System reserviert für jede dieser Verbindungen bestimmte Ressourcen, wodurch es seine gesamten Ressourcen verbraucht und nicht auf Verbindungsanfragen anderer Quellen reagiert. Für diesen Angriff können Sie durch **Anzahl der Verbindungen** die Anzahl der Verbindungen festlegen, die ein Remote-Computer innerhalb des durch **Zeit (Sek)** angegebenen Zeitraums zu öffnen versucht.

- ***UDP Flood**:* Bei diesem Angriff wird ein UDP-Paket gesendet, das auf Grund seiner Struktur endlos zwischen dem angegriffenen Computer und einer dem angegriffenen Computer frei zugänglichen Adresse hin- und hergeschickt wird. Dies führt auf beiden Computern zum Verlust von Ressourcen und erhöht die Belastung des Verbindungskanals. Für diesen Angriff können Sie durch **Anzahl der UPD-Pakete** die Anzahl der eingehenden UDP-Pakete festlegen, die ein Remote-Computer innerhalb des durch **Zeit (Sek)** angegebenen Zeitraums zu senden versucht.

- ***ICMP Flood**:* Bei diesem Angriff werden große Mengen von ICMP-Paketen an den angegriffenen Computer gesendet. Dies führt zu einer stark erhöhten Prozessorbelastung, da der Computer auf jedes Paket reagiert. Für diesen Angriff können Sie durch **Anzahl der ICMP-Pakete** die Anzahl der eingehenden ICMP-Pakete festlegen, die ein Remote-Computer innerhalb des durch **Zeit (Sek)** angegebenen Zeitraums zu senden versucht.

- ***Helkern**:* Bei diesem Angriff werden spezielle UDP-Pakete mit ausführbarem schädlichem Code an den angegriffenen Computer gesendet. Der Angriff führt zur Verlangsamung der Internetfunktionen.

- ***SmbDie**:* Bei diesem Angriff wird versucht, eine Verbindung nach SMB-Protokoll aufzubauen; bei erfolgreicher Verbindung wird an den angegriffenen Computer ein spezielles Paket gesendet, das versucht, den

Puffer zu überfüllen. Als Folge wird der Computer neu gestartet. Dieser Angriff gefährdet die Betriebssysteme Windows 2k/XP/NT

- Bei einem Angriff durch ***Lovesan*** wird versucht, auf Ihrem Computer Sicherheitslücken im Service DCOM RPC der Betriebssysteme Windows NT 4.0/NT 4.0 Terminal Services Edition/2000/XP/Server(tm) 2003 zu ermitteln. Sind solche Schwachstellen auf dem Computer vorhanden, dann wird ein Programm mit schädlichen Funktionen gesendet, das es erlaubt, auf Ihrem Computer beliebige Manipulationen vorzunehmen.

KAPITEL 7. ANSICHT DER ARBEITSERGEBNISSE

7.1. Informationen über den aktuellen Status

Die Netzwerk-Aktivität aller Anwendungen, die auf Ihrem Computer installiert sind, wird von dem Programm Kaspersky Anti-Hacker kontinuierlich überwacht. Sie können die Informationen über die Netzwerk-Aktivität in folgender Form anzeigen:

- **Liste der aktiven Anwendungen**. Die gesamte Netzwerk-Aktivität wird nach den Anwendungen gruppiert, die eine Aktivität initiieren. Für jede Anwendung wird eine Liste der Ports und Verbindungen angegeben, über die diese Anwendung verfügt.

- **Liste der aktiven Verbindungen**. Alle ein- und ausgehenden Verbindungen, Adressen von Remote-Computern und Portnummern werden dargestellt.

- **Liste der offenen Ports**. Diese Liste enthält die offenen Ports auf Ihrem Computer.

7.1.1. Liste der aktiven Anwendungen

Wenn Sie überprüfen möchten, welche Netzwerk-Anwendungen im Moment auf Ihrem Computer aktiv sind,

wählen Sie im Menü **Ansicht** den Punkt **Anzeigen**, und im folgenden Untermenü den Punkt **Aktive Anwendungen** (s. Abb. 36). Um diese Liste zu öffnen, können Sie auch die Schaltfläche in der Symbolleiste verwenden.

Danach erscheint das Dialogfenster **Liste der aktiven Anwendungen** auf dem Bildschirm.

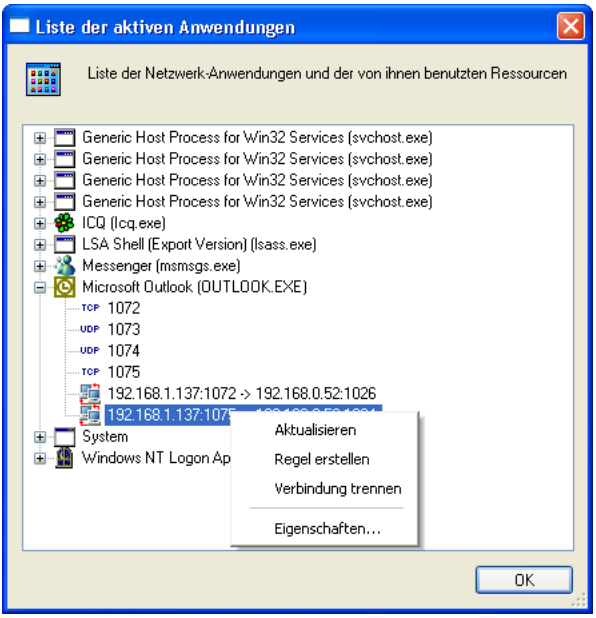


Abbildung 36. Dialogfenster **Liste der aktiven Anwendungen**

Mit Hilfe dieses Dialogfensters können Sie die Liste der aktiven Anwendungen und der zugehörigen Netzwerk-Ressourcen ansehen. Die Anwendungen sind nach Namen geordnet, was die Orientierung in der Liste erleichtert. Links des Namens jeder Anwendung befindet sich deren Symbol.

Wird die Zeile mit dem Anwendungsnamen aufgeklappt, dann ist die Liste der offenen Ports und der hergestellten Verbindungen für jede konkrete Anwendung zu sehen:

- Ein offener Port wird in Abhängigkeit vom Typ des Ports durch das Symbol **TCP** oder **UDP** markiert. Rechts davon ist die Portnummer angegeben.

- Eine Verbindung wird durch das Symbol markiert, wenn Ihr Computer die Verbindung initiiert hat, oder durch das Symbol , wenn die Verbindung von außen hergestellt wurde. Rechts des Symbols werden die Verbindungsparameter angegeben:
  `<Adresse des Initiators>:<Port des Initiators>` → `<Zieladresse>:<Zielport>`

Die Liste der aktiven Anwendungen wird automatisch zwei Mal pro Sekunde aktualisiert.

Die Liste verfügt über ein Kontextmenü, das aus folgenden Punkten besteht:

- **Aktualisieren** – Manuelle Aktualisierung der Informationen über aktive Netzwerk-Anwendungen.

- **Regel erstellen** – Erstellen einer Regel auf Basis eines aus der Liste gewählten Ports oder Verbindung. Das Programm ruft den Regelassistenten für Anwendungen auf und fügt die Daten über die von Ihnen gewählte Portnummer oder Verbindung ein.

- **Verbindung trennen** – Trennen einer bestehenden Verbindung, die in der Liste gewählt wurde (dieser Punkt steht nur bei Auswahl von Verbindungen zur Verfügung).

Vorsicht! Bei der manuellen Trennung einer Verbindung kann es bei bestimmten Anwendungen zu Funktionsstörungen kommen.

- **Eigenschaften...** – Anzeige von detaillierten Informationen über eine aus der Liste gewählte Anwendung (s. Abb. 37), Verbindung (s. Abb. 39) oder einen Port (s. Abb. 41).

Die Tabelle kann mehrere Zeilen mit identischen Anwendungsnamen enthalten. Das weist darauf hin, dass eine Anwendung mehrfach gestartet wurde. Bitte beachten Sie, dass nach dem Öffnen von Zeilen mit gleichen Namen unterschiedliche Listen der offenen Ports und aktiven Verbindungen angezeigt werden können.

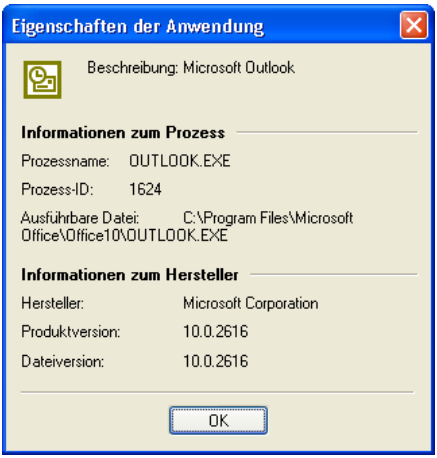


Abbildung 37. Dialogfenster **Eigenschaften der Anwendung**

Im oberen Teil des Dialogfensters **Eigenschaften der Anwendung** befindet sich der Abschnitt **Informationen zur Anwendung**:

- **Name der Anwendung** – Name der ausführbaren Datei
- **ID der Anwendung** – Identifikator der Anwendung
- **Ausführbare Datei** – vollständiger Pfad der ausführbaren Datei

Im unteren Teil der Datentabelle befindet sich der Abschnitt **Informationen zum Hersteller**:

- **Hersteller** – Informationen über die Herstellerfirma des Programms
- **Produktversion** – Versionsnummer des Programms
- **Dateiversion** – Versionsnummer der ausführbaren Datei

7.1.2. Liste der aktiven Verbindungen

Zum Öffnen einer Liste der aktiven Verbindungen

wählen Sie im Menü **Ansicht** den Punkt **Anzeigen**, und im folgenden Untermenü den Punkt **Aktive Verbindungen** (s. Abb. 38). Zum Öffnen dieser Liste können Sie auch die Schaltfläche in der Symbolleiste verwenden.

Danach erscheint das Dialogfenster **Aktive Verbindungen** auf dem Bildschirm.

Jede Zeile der Liste entspricht einer Verbindung. Eine Verbindung wird durch das Symbol markiert, wenn Ihr Computer die Verbindung initiiert hat, oder durch das Symbol , wenn die Verbindung von außen hergestellt wurde.

Für jede Verbindung werden folgende Werte angezeigt:

- **Remote-Adresse** – Adresse und Port des Remote-Computers, mit dem eine Verbindung hergestellt wurde.
- **Lokale Adresse** – Adresse und Port Ihres Computers
- **Anwendung** – Die Anwendung, welche die Verbindung initiiert hat.

Die Liste kann nach den genannten Parametern sortiert werden.

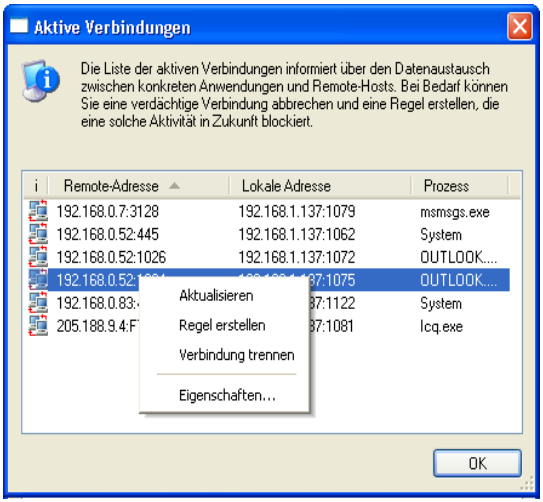


Abbildung 38. Dialogfenster **Aktive Verbindungen**

Die Liste der aktiven Verbindungen wird automatisch zwei Mal pro Sekunde aktualisiert.

Bei Bedarf können Sie unerwünschte Verbindungen trennen und/oder Regeln erstellen, die solche Verbindungen in Zukunft verbieten. Verwenden Sie dazu das Kontextmenü:

- **Aktualisieren** – Manuelle Aktualisierung der Informationen über aktive Verbindungen
- **Regel erstellen** – Erstellen einer Regel auf Basis einer aus der Liste gewählten Verbindung. Das Programm ruft den Regelassistenten für Anwendungen auf und fügt die Daten über die von Ihnen gewählte Verbindung ein.
- **Verbindung trennen** – Trennen einer aus der Liste gewählten Verbindung

Vorsicht! Bei der manuellen Trennung einer Verbindung kann es bei bestimmten Anwendungen zu Funktionsstörungen kommen.

- **Eigenschaften...** – Anzeige von detaillierten Informationen über eine aus der Liste gewählte Verbindung (s. Abb. 39)

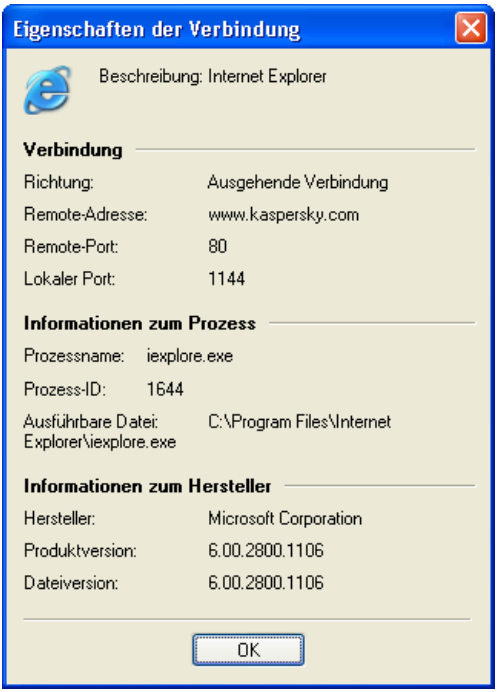


Abbildung 39. Dialogfenster **Eigenschaften der Verbindung**

Der Abschnitt **Verbindung** des Dialogfensters **Eigenschaften der Verbindung** enthält folgende Angaben:

- **Richtung** – Gibt an, ob es sich um eine eingehende oder ausgehende Verbindung handelt.
- **Remote-Adresse** – Symbolischer Name oder IP-Adresse des Remote-Computers
- **Remote-Port** – Nummer des Remote-Ports
- **Lokaler Port** – Nummer des lokalen Ports

Darunter befinden sich die Abschnitte **Informationen zur Anwendung** und **Informationen zum Hersteller** (s. Pkt. 7.1.1 auf S. 73).

7.1.3. Liste der offenen Ports

Zum Öffnen einer Liste der offenen Ports

wählen Sie im Menü **Ansicht** den Punkt **Anzeigen**, und im folgenden Untermenü den Punkt **Offene Ports** (s. Abb. 40). Um diese Liste zu öffnen, können Sie auch die Schaltfläche in der Symbolleiste verwenden.

Danach erscheint das Dialogfenster **Offene Ports** auf dem Bildschirm.

Jede Zeile der Liste entspricht einem offenen Port. Ein Port wird in Abhängigkeit seines Typs durch das **TCP** oder **UDP** markiert.

Für jeden offenen Port werden folgende Werte angezeigt:

- **Lokaler Port** – Nummer des Ports
- **Anwendung** – Die Anwendung, die den Port geöffnet hat.
- **Pfad** – vollständiger Pfad des ausführbaren Moduls

Die Liste kann nach den genannten Parametern sortiert werden.

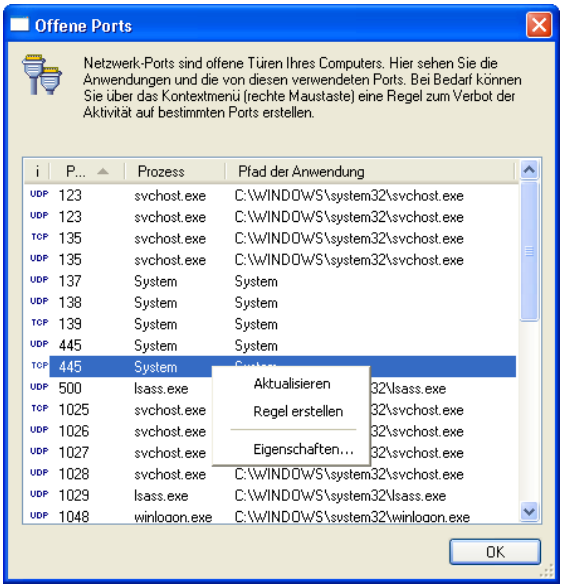

Offene Ports
Netzwerk-Ports sind offene Türen Ihres Computers. Hier sehen Sie die Anwendungen und die von diesen verwendeten Ports. Bei Bedarf können Sie über das Kontextmenü (rechte Maustaste) eine Regel zum Verbot der Aktivität auf bestimmten Ports erstellen.
i
P...
Prozess
Pfad der Anwendung
UDP 123 svchost.exe C:\WINDOWS\system32\svchost.exe
UDP 123 svchost.exe C:\WINDOWS\system32\svchost.exe
TCP 135 svchost.exe C:\WINDOWS\system32\svchost.exe
UDP 135 svchost.exe C:\WINDOWS\system32\svchost.exe
UDP 137 System System
UDP 138 System System
TCP 139 System System
UDP 445 System System
TCP 445 System
UDP 500 lsass.exe
TCP 1025 svchost.exe
UDP 1026 svchost.exe
UDP 1027 svchost.exe
UDP 1028 svchost.exe C:\WINDOWS\system32\svchost.exe
UDP 1029 lsass.exe C:\WINDOWS\system32\lsass.exe
UDP 1048 winlogon.exe C:\WINDOWS\system32\winlogon.exe
Aktualisieren
Regel erstellen
Eigenschaften...
OK

Abbildung 40. Dialogfenster **Offene Ports**

Die Liste der offenen Ports wird automatisch zwei Mal pro Sekunde aktualisiert.

Bei Bedarf können Sie eine Regel erstellen, die in Zukunft Verbindungen auf einem bestimmten Port verbietet. Verwenden Sie dazu das Kontextmenü:

- **Aktualisieren** – Manuelle Aktualisierung der Informationen über die offenen Ports

- **Regel erstellen** – Erstellen einer Regel auf Basis eines aus der Liste gewählten Ports. Das Programm ruft den Regelassistenten für Anwendungen auf und fügt die Daten über den von Ihnen gewählten Port ein.

- **Eigenschaften...** – Anzeige von detaillierten Informationen über einen aus der Liste gewählten Port (s. Abb. 41)

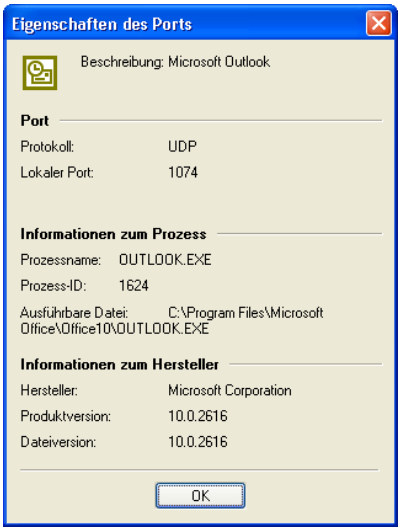


Abbildung 41. Dialogfenster **Eigenschaften des Ports**

Der Abschnitt **Port** des Dialogfensters **Eigenschaften des Ports** enthält folgende Angaben:

- **Protokoll** – Name des Protokolls
- **Lokaler Port** – Nummer des lokalen Ports

Darunter befinden sich die Abschnitte **Informationen zur Anwendung** und **Informationen zum Hersteller** (s. Pkt. 7.1.1 auf S. 73).

7.2. Arbeit mit den Protokollen

Netzwerk-Ereignisse, die auf Ihrem Computer eintreten, werden in *Protokolle* eingetragen und dort gespeichert. Es sind drei Protokolltypen für folgende Ereigniskategorien vorgesehen:

- **Sicherheit**. In diesem Protokoll werden Informationen über die letzten Angriffe auf Ihren Computer gespeichert (s. Pkt. 6.5 auf S. 69).

- **Aktivität der Anwendungen**. In diesem Protokoll werden Ereignisse eingetragen, deren Aufzeichnung Sie im Regelassistenten für Anwendungen festgelegt haben (s. Pkt. 6.3.2.3 auf S. 59).

- **Paketfilterung**. In diesem Protokoll werden Ereignisse eingetragen, deren Aufzeichnung Sie im Regelassistenten für Paketfilterung festgelegt haben (s. Pkt. 6.4.2.2 auf S. 68).

Für die Arbeit mit allen drei Protokollen dient ein einheitliches Fenster (das *Fenster Protokolle*).

Die maximale Größe der Protokolle kann begrenzt werden. Außerdem können Sie wählen, ob das Protokoll bei jedem Programmstart gelöscht werden soll oder ob die Ergebnisse mehrerer Sitzungen gespeichert werden sollen (s. Pkt. 7.2.4 auf S. 88).

Falls erwünscht, können Sie das Protokoll manuell löschen.

Außerdem können Sie das Protokoll in einer Datei auf der Festplatte speichern.

7.2.1. Öffnen des Protokollfensters

Um das Protokollfenster zu öffnen,

wählen Sie im Menü **Ansicht** den Punkt **Protokolle**, und im folgenden Menü den Punkt für den gewünschten Protokolltyp.

Danach erscheint das Protokollfenster auf dem Bildschirm (s. Abb. 42).

7.2.2. Benutzeroberfläche des Protokollfensters

Das Protokollfenster besteht aus folgenden Elementen:

- Hauptmenü

- Protokolltabelle

- Verknüpfungen mit den einzelnen Registerkarten zur Auswahl des gewünschten Protokolltyps

7.2.2.1. Hauptmenü

Im oberen Bereich des Hauptfensters befindet sich das *Hauptmenü*.

Tabelle 4

Menüpunkt	**Funktion**
Datei ⟶ Speichern in Datei	Speichern des aktuellen Protokolls in einer Datei
Datei ⟶ Schließen	Schließen des Protokollfensters
Hilfe ⟶ Inhalt…	Öffnen des Hilfesystems
Hilfe ⟶ Kaspersky Anti-Hacker im Internet	Öffnen der Webseite von Kaspersky Lab
Hilfe ⟶ Über das Programm...	Anzeige von Informationen über das Programm

7.2.2.2. Protokolltabelle

In der Protokolltabelle wird das Protokoll des gewählten Typs angezeigt. Sie können die Tabelle mit Hilfe der vertikalen Bildlaufleiste ansehen.

Die Protokolltabelle verfügt über ein Kontextmenü, das standardmäßig aus zwei Punkten besteht und in Abhängigkeit des gewählten Protokolls zusätzliche Punkte enthält:

- **Protokoll löschen** – Löschen des gewählten Protokolls

- **Auto-Bildlauf für Protokoll** – Im sichtbaren Bereich der Protokolltabelle immer den Eintrag über das letzte Ereignis anzeigen.

- **Dieses Ereignis nicht protokollieren** – Einträge über das markierte Ereignis in Zukunft nicht mehr protokollieren. Dieser Punkt steht für alle Protokolle zur Verfügung, außer für das Protokoll Sicherheit.

- **Regel erstellen** – Erstellen einer Regel auf Basis des markierten Ereignisses. Beim Erstellen der Regel wird dieser in der Regelliste die höchste Priorität verliehen.

7.2.2.3. Verknüpfungen mit den Registerkarten

Die Verknüpfungen mit den Registerkarten dienen der Auswahl des gewünschten Protokolls:

- Sicherheit

- Aktivität der Anwendungen

- Paketfilterung

7.2.3. Auswahl des Protokolls

7.2.3.1. Das Protokoll "Sicherheit"

Sie können das Protokoll "Sicherheit" öffnen, das eine Liste aller erkannten Angriffsversuche auf Ihren Computer enthält (s. Pkt. 6.5 auf S. 69).

Um das Protokoll "Sicherheit" zu öffnen,

wählen Sie im Menü **Ansicht** den Punkt **Protokolle**, und im folgenden Untermenü den Punkt **Sicherheit**.

Danach wird das Fenster **Protokolle** auf der Seite **Sicherheit** geöffnet (s. Abb. 42). Das Protokoll enthält die Spalten:

- **Datum und Uhrzeit** – Datum und Uhrzeit des Angriffsversuchs auf Ihren Computer

- **Ereignis-Beschreibung** – Beschreibung des Netzwerk-Angriffs: Name des Angriffs und Adresse des angreifenden Computers, falls diese ermittelt werden konnte.

Die Liste der Ereignisse kann nur nach Datum und Uhrzeit sortiert werden.

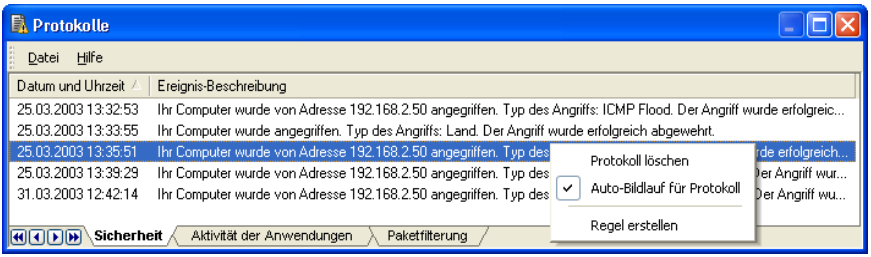

Protokolle
Datei
Hilfe
Datum und Uhrzeit
Ereignis-Beschreibung
25.03.2003 13:32:53 Ihr Computer wurde von Adresse 192.168.2.50 angegriffen. Typ des Angriffs: ICMP Flood. Der Angriff wurde erfolgreic...
25.03.2003 13:33:55 Ihr Computer wurde angegriffen. Typ des Angriffs: Land. Der Angriff wurde erfolgreich abgewehrt.
25.03.2003 13:35:51 Ihr Computer wurde von Adresse 192.168.2.50 angegriffen. Typ des
25.03.2003 13:39:29 Ihr Computer wurde von Adresse 192.168.2.50 angegriffen. Typ des
31.03.2003 12:42:14 Ihr Computer wurde von Adresse 192.168.2.50 angegriffen. Typ des
Protokoll löschen
Auto-Bildlauf für Protokoll
Regel erstellen
Sicherheit
Aktivität der Anwendungen
Paketfilterung

Abbildung 42. Das Sicherheitsprotokoll

7.2.3.2. Das Protokoll "Aktivität der Anwendungen"

Sie können das Protokoll über die Aktivität von Anwendungen öffnen, für die in den Regeln für Anwendungen die Protokollierung festgelegt wurde (s. Pkt. 6.3.2.3 auf S. 59).

Um das Protokoll "Aktivität der Anwendungen" zu öffnen,

wählen Sie im Menü **Ansicht** den Punkt **Protokolle**, und im folgenden Untermenü den Punkt **Aktivität der Anwendungen**.

Danach wird das Fenster **Protokolle** auf der Seite **Aktivität der Anwendungen** geöffnet (s. Abb. 43). Das Protokoll enthält die Spalten:

- **Datum und Uhrzeit** – Datum und Uhrzeit des betreffenden Ereignisses
- **Anwendung** – Name der Anwendung und Pfad der ausführbaren Datei
- **Beschreibung der Aktivität** – Kommentar zu der betreffenden Aktivität
- **Lokale Adresse** – lokale Adresse

- **Remote-Adresse** – Remote-Adresse

Die Liste der Ereignisse kann nur nach Datum und Uhrzeit sortiert werden.

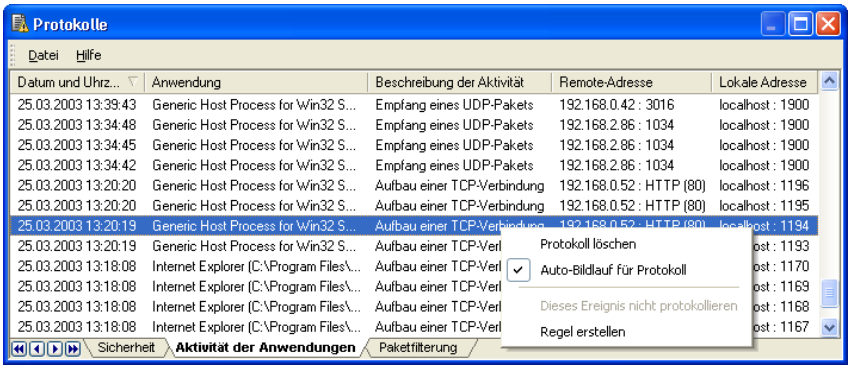

Protokolle
Datei
Hilfe
Datum und Uhrz...
Anwendung
Beschreibung der Aktivität
Remote-Adresse
Lokale Adresse
25.03.2003 13:39:43 Generic Host Process for Win32 S... Empfang eines UDP-Pakets 192.168.0.42 : 3016 localhost : 1900
25.03.2003 13:34:48 Generic Host Process for Win32 S... Empfang eines UDP-Pakets 192.168.2.86 : 1034 localhost : 1900
25.03.2003 13:34:45 Generic Host Process for Win32 S... Empfang eines UDP-Pakets 192.168.2.86 : 1034 localhost : 1900
25.03.2003 13:34:42 Generic Host Process for Win32 S... Empfang eines UDP-Pakets 192.168.2.86 : 1034 localhost : 1900
25.03.2003 13:20:20 Generic Host Process for Win32 S... Aufbau einer TCP-Verbindung 192.168.0.52 : HTTP (80) localhost : 1196
25.03.2003 13:20:20 Generic Host Process for Win32 S... Aufbau einer TCP-Verbindung 192.168.0.52 : HTTP (80) localhost : 1195
25.03.2003 13:20:19 Generic Host Process for Win32 S... Aufbau einer TCP-Verbindung
25.03.2003 13:20:19 Generic Host Process for Win32 S... Aufbau einer TCP-Verl
25.03.2003 13:18:08 Internet Explorer (C:\Program Files\... Aufbau einer TCP-Verl
25.03.2003 13:18:08 Internet Explorer (C:\Program Files\... Aufbau einer TCP-Verl
25.03.2003 13:18:08 Internet Explorer (C:\Program Files\... Aufbau einer TCP-Verl
25.03.2003 13:18:08 Internet Explorer (C:\Program Files\... Aufbau einer TCP-Verl
Protokoll löschen
Auto-Bildlauf für Protokoll
Dieses Ereignis nicht protokollieren
Regel erstellen
Sicherheit
Aktivität der Anwendungen
Paketfilterung

Abbildung 43. Das Protokoll über Aktivität der Anwendungen

7.2.3.3. Das Protokoll "Paketfilterung"

Sie können das Protokoll über Aktivitäten auf Paketebene öffnen, deren Protokollierung in den Regeln für Paketfilterung festgelegt wurde (s. Pkt. 6.4.2.2 auf S. 68).

Um das Protokoll "Paketfilterung" zu öffnen,

wählen Sie im Menü **Ansicht** den Punkt **Protokolle**, und im folgenden Untermenü den Punkt **Paketfilterung**.

Danach wird das Fenster **Protokolle** auf der Seite **Paketfilterung** geöffnet (s. Abb. 44). Das Protokoll enthält die Spalten:

- **Datum und Uhrzeit** – Datum und Uhrzeit des betreffenden Ereignisses
- **Richtung** – eingehendes oder ausgehende Paket
- **Protokoll** – Name des Protokolls
- **Lokale Adresse** – lokale Adresse

- **Remote-Adresse** – Remote-Adresse
- **Verwendete Regel** – Name der angewandten Regel

Erlaubnisregeln werden schwarz dargestellt, Verbotsregeln rot.

Die Liste der Ereignisse kann nur nach Datum und Uhrzeit sortiert werden.

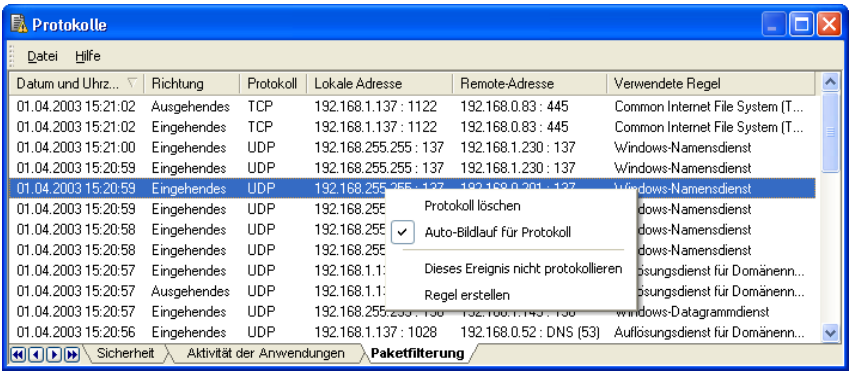

Protokolle
Datei Hilfe
Datum und Uhrz... Richtung Protokoll Lokale Adresse Remote-Adresse Verwendete Regel
01.04.2003 15:21:02 Ausgehendes TCP 192.168.1.137 : 1122 192.168.0.83 : 445 Common Internet File System (T...
01.04.2003 15:21:02 Eingehendes TCP 192.168.1.137 : 1122 192.168.0.83 : 445 Common Internet File System (T...
01.04.2003 15:21:00 Eingehendes UDP 192.168.255.255 : 137 192.168.1.230 : 137 Windows-Namensdienst
01.04.2003 15:20:59 Eingehendes UDP 192.168.255.255 : 137 192.168.1.230 : 137 Windows-Namensdienst
01.04.2003 15:20:59 Eingehendes UDP
01.04.2003 15:20:59 Eingehendes UDP
01.04.2003 15:20:58 Eingehendes UDP
01.04.2003 15:20:58 Eingehendes UDP
01.04.2003 15:20:57 Eingehendes UDP
01.04.2003 15:20:57 Ausgehendes UDP
01.04.2003 15:20:57 Eingehendes UDP
01.04.2003 15:20:56 Eingehendes UDP 192.168.1.137 : 1028 192.168.0.52 : DNS (53) Auflösungsdienst für Domänenn...
Protokoll löschen
Auto-Bildlauf für Protokoll
Dieses Ereignis nicht protokollieren
Regel erstellen
Sicherheit
Aktivität der Anwendungen
Paketfilterung

Abbildung 44. Das Protokoll über Paketfilterung

7.2.4. Konfiguration der Protokollparameter

Zur Konfiguration der Protokollparameter

wählen Sie im Menü **Service** den Punkt **Einstellungen** und gehen Sie auf die Registerkarte **Protokolle** (s. Abb. 45).

Sie können Werte für die folgenden zwei Parameter festlegen:

- **Protokolle bei Programmstart löschen** – bei Programmstart alle drei Protokolle löschen
- **Maximale Protokollgröße festlegen (KB)** – Festlegen der maximalen Größe einer Protokolldatei. Der entsprechende Wert wird in dem unter dem Kontrollkästchen angebrachten Eingabefeld angegeben. Beim Erreichen der maximalen Größe werden neue Einträge dem Protokoll hinzugefügt, während die ältesten Einträge gelöscht werden.

Bitte beachten Sie, dass mit Hilfe dieser Option die Größe eines EINZELNEN Protokolls festgelegt wird, nicht die Größe aller drei Protokolle. Bei der Berechnung des für die korrekte Funktion des Programms auf der Festplatte erforderlichen Speicherplatzes ist der Wert mit drei zu multiplizieren.

Abbildung 45. Registerkarte **Protokolle** des Dialogfensters **Einstellungen**

7.2.5. Speichern einer Protokolldatei auf der Festplatte

*Um ein im Fenster **Protokolle** gewähltes Protokoll zu speichern,*

wählen Sie im Menü **Datei** den Punkt **Speichern in Datei**. Geben Sie im folgenden Dialogfenster den gewünschten Dateinamen an. Das Protokoll wird im Textformat gespeichert.

ANHANG A. KASPERSKY LAB

Die Firma Kaspersky Lab wurde 1997 gegründet. Heute sind wir das bekannteste Unternehmen für Datenschutz-Software in Russland und bieten eine breite Palette an Programmen zum Schutz vor Viren, unerwünschten E-Mails (Spam) und Hackerangriffen.

Kaspersky Lab ist ein international operierender Konzern. Unser Firmensitz befindet sich in Russland, regionale Vertretungen bestehen in Großbritannien, Frankreich, Deutschland, Japan, den Benelux-Staaten, China, Polen, Rumänien und den USA (Kalifornien). In Frankreich wurde jüngst ein neues Subunternehmen eröffnet – das Europäische Zentrum für Antivirenforschung. Unser Partnernetzwerk vereint weltweit mehr als 500 Firmen.

Kaspersky Lab heute – das sind mehr als 250 hoch qualifizierte Fachleute, von denen neun den Titel eines MBA sowie fünfzehn einen Doktortitel besitzen und zwei Mitglieder der international angesehenen Computer Anti-virus Researcher's Organization (CARO) sind.

Das wertvollste Potenzial des Unternehmens sind einmaliges Know-how und Erfahrung, gesammelt durch unsere Mitarbeiter im Laufe von vierzehn Jahren ständigen Kampfes mit Computerviren. Durch ständige Analyse der Entwicklung im Bereich Computerviren sind wir in der Lage, neue Tendenzen für gefährliche Programme vorherzusehen und den Anwendern frühzeitig zuverlässige Lösungen zum Schutz vor neuen Attacken anzubieten. Dieser Vorteil ist die Basis für den Erfolg der Programme und Services von Kaspersky Lab. Wir sind unserer Konkurrenz stets einen Schritt voraus und garantieren maximale Sicherheit zum Wohle unserer Klientel.

In jahrelangen Bemühungen ist es uns gelungen, die Marktführerschaft in der Entwicklung von Virenschutzprogrammen zu erobern. Viele moderne Standards für Virenschutzprogramme wurden erstmals von Kaspersky Lab entwickelt. Unser führendes Produkt, **Kaspersky Anti-Virus**, garantiert zuverlässigen Schutz für alle Objekte, die Virenattacken ausgesetzt sind: Computer-Arbeitsplätze, Dateiserver, Mail Exchanger, Firewalls und Internet-Gateways, Handheld-Computer. Die bequeme Handhabung erlaubt einen größtenteils automatisierten Virenschutz in den Firmennetzwerken der Anwender. Viele westliche Softwarehersteller verwenden in ihren Programmen die Quellcodes von **Kaspersky Anti-Virus**, darunter: Nokia ICG (USA), F-Secure (Finnland), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Die Kunden von Kaspersky Lab erhalten ein breites Spektrum zusätzlicher Dienstleistungen, welche die störungsfreie Funktion der Produkte und die präzise Abstimmung auf spezifische Anforderungen garantieren. Wir planen, implementieren und warten Antivirenkomplexe für Unternehmen. Unsere Antiviren-Datenbanken werden alle drei Stunden aktualisiert. Unseren Anwendern bieten wir rund um die Uhr technische Unterstützung in mehreren Sprachen.

A.1. Andere Produkte von Kaspersky Lab

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal schützt Ihren daheim genutzten Computer unter Windows 98/ME, 2000/NT/XP vor allen bekannten Virenarten einschließlich potentiell gefährlicher Software. Das Programm kontrolliert laufend sämtliche Kanäle für möglichen Virenbefall – E-Mail, Internet, Disketten, CDs u.a. Das einmalige heuristische Datenanalyse-System neutralisiert auf wirksame Weise unbekannte Viren. Folgende Varianten für die Arbeit des Programms lassen sich unterscheiden (Diese können separat oder gemeinsam verwendet werden):

- **Echtzeitschutz des Computers** – Virensuche bei allen Objekten, die auf dem Computer gestartet, geöffnet und gespeichert werden.

- **Scan auf Befehl** – Untersuchung und Säuberung sowohl des gesamten Computers als auch einzelner Laufwerke, Dateien oder Verzeichnisse. Sie können diese Untersuchung selbständig starten oder den regelmäßigen automatischen Start der Untersuchung konfigurieren.

Kaspersky Anti-Virus® Personal untersucht nun Objekte, die während einer vorhergehenden Untersuchung gescannt wurden und seitdem nicht verändert wurden, nicht erneut. Dies gilt sowohl für den Echtzeitschutz als auch für den Scan auf Befehl. Dadurch **erhöht sich die Operationsgeschwindigkeit des Programms wesentlich**.

Das Programm schafft eine zuverlässige Barriere gegen das Eindringen von Viren über E-Mails. Kaspersky Anti-Virus® Personal führt automatisch die Untersuchung und Säuberung des gesamten nach den Protokollen POP3 und SMTP ein- und ausgehenden E-Mailverkehrs durch und bietet die effiziente Untersuchung von Mail-Datenbanken.

Das Programm unterstützt mehr als siebenhundert Formate für Archive und komprimierte Dateien, überprüft deren Inhalt auf Viren und eliminiert gefährliche Codes aus **ZIP, CAB, RAR, ARJ** -Archiven.

Die komfortable Bedienung des Programms wird durch die Auswahl zwischen drei voreingestellten Sicherheitsstufen realisiert: **Maximale Sicherheit**, **Empfohlen** und **Maximales Tempo**.

Die Antiviren-Datenbanken werden alle drei Stunden aktualisiert. Die vollständige Übertragung wird auch bei Unterbrechung oder Wechsel der Internetverbindung garantiert.

Kaspersky Anti-Virus® Personal Pro

Dieses Programmpaket wurde speziell entwickelt, um den vollwertigen Antivirenschutz für Heimcomputer unter den Betriebssystemen Windows 98/ME, Windows 2000/NT, Windows XP, sowie mit MS Office Anwendungen der Business-Edition zu gewährleisten. Kaspersky Anti-Virus® Personal Pro verfügt über eine Funktion zum täglichen Download von Updates für Antiviren-Datenbanken und Programmmodule. Das einmalige heuristische System zur Datenanalyse der zweiten Generation erlaubt, unbekannte Viren wirksam zu neutralisieren. Die einfache und praktische Benutzeroberfläche ermöglicht das schnelle Anpassen der Einstellungen und sorgt für größtmöglichen Komfort im Umgang mit dem Programm.

Kaspersky Anti-Virus® Personal Pro bietet:

- **die Antiviren-Untersuchung** der lokalen Laufwerke **auf Befehl des Benutzers**.
- **die automatische Untersuchung im Echtzeitmodus** auf Viren in allen verwendeten Dateien.
- **einen E-Mail-Filter**, der automatisch die Untersuchung und Desinfektion des gesamten nach den Protokollen POP3 und SMTP ein- und ausgehenden E-Mail-Verkehrs vornimmt und Mail-Datenbanken effektiv auf Viren untersucht.
- **Behaviour Blocker**, der hundertprozentigen Schutz vor Makroviren für MS Office Anwendungen garantiert.
- **die Antiviren-Untersuchung** von über 900 Versionen archivierter und gepackter Dateiformate und gewährleistet die automatische Antiviren-Untersuchung des Inhalts, sowie das Entfernen von schädlichem Code aus Archivdateien der Formate **ZIP**, **CAB**, **RAR**, **ARJ**.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker ist eine persönliche Firewall, die Ihren Computer unter Windows vollständig gegen unberechtigten Zugriff auf Daten und gegen Hackerangriffe über das Internet oder lokale Netzwerke abschirmt.

Kaspersky® Anti-Hacker verfolgt die Netzaktivitäten über ein TCP/IP-Protokoll für sämtliche Anwendungen auf Ihrem Computer. Falls für eine Anwendung verdächtige Aktivitäten registriert werden, gibt das Programm eine Warnmeldung aus und blockiert, falls erforderlich, den Zugriff über das Netz für die entsprechende Anwendung, so dass die auf dem Computer gespeicherten Daten geschützt bleiben.

Durch Verwendung der SmartStealth™-Technologie wird das Aufspüren des Computers von außerhalb erheblich erschwert: da der Computer unsichtbar bleibt, ist er vor Hackerangriffen geschützt, ohne dass jedoch Ihre eigene Kommunikations- und Arbeitsfähigkeit über das Internet beeinträchtigt wird. Das Programm gewährleistet angemessenen Schutz aber auch den standardmäßigen Zugriff auf die Daten des Computers.

Kaspersky® Anti-Hacker blockiert weiterhin die am weitesten verbreiteten Formen von Netzattacken durch Hacker sowie Versuche zum Ausspähen einzelner Ports.

Das Programm bietet vereinfachte Steuerungsmöglichkeiten über fünf verschiedene Sicherheitsstufen. Als Standardeinstellung wird eine lernfähige Systemkonfiguration verwendet, so dass die Sicherheitseinstellungen an Ihre individuelle Reaktion auf verschiedene Ereignisse angepasst werden können. Dadurch wird es möglich, die Konfiguration der Firewall individuell auf bestimmte Anwender und einzelne Computer abzustimmen.

Kaspersky® Security für PDA

Kaspersky® Security für PDA gewährleistet zuverlässigen Virenschutz für Daten auf Handheld-PCs unter Palm OS oder Windows CE sowie für Daten, die von einem gewöhnlichen PC oder Erweiterungsspeichern, von CD-ROM oder aus Datenbanken übernommen werden. Das Programm umfasst eine optimale Auswahl an Virenschutz-Komponenten:

- **einen Virenscanner**, der eine Untersuchung der Daten (sowohl im Speicher des PDA selbst, als auch auf beliebigen Speicher-Erweiterungskarten) auf Anforderung des Anwenders ausführt;

- **den Antivirus-Monitor**, der während der Synchronisation über HotSync™ und während des Datenaustausches mit anderen PDA Virenprogramme blockiert.

Weiterhin schützt das Programm die auf dem PDA gespeicherten Informationen vor unberechtigtem Zugriff durch Verschlüsselung des Zugriffs auf das Gerät selbst wie auch auf die im Speicher des PDA und auf Speicherkarten enthaltenen Daten.

Kaspersky Anti-Virus® Business Optimal

Dieses Programmpaket ist die ultimative Lösung zum Schutz vor Computerviren für Unternehmen kleiner und mittlerer Größe.

Kaspersky Anti-Virus® Business Optimal bietet Rundumschutz[1] vor Viren für:

- *Computerarbeitsplätze* unter Windows 98/Me, Windows 2000/NT/XP Workstation, Linux.
- *Dateiserver* unter Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD und OpenBSD, Linux.
- *Mailsysteme* vom Typ Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail und Qmail.
- *Internet-Firewalls:* CheckPoint Firewall –1; MS ISA Server.

Kaspersky Anti-Virus® Busines Optimal beinhaltet außerdem ein zentrales Installations- und Administrationssystem, Kaspersky® Administration Kit.

Sie selbst wählen die geeigneten Virenschutzprogramme in Abhängigkeit von den in Ihrem Unternehmen verwendeten Betriebssystemen und Anwendungen.

Kaspersky® Corporate Suite

Kaspersky® Corporate Suite ist eine integrierte Softwarelösung zum Datenschutz für Ihr gesamtes Firmennetzwerk ohne Einschränkungen hinsichtlich Größe und Struktur. Die enthaltenen Programmkomponenten schützen jeden Punkt ihres firmeninternen Netzes. Sie sind kompatibel mit den meisten heute verbreiteten Betriebssystemen und Anwendungen, über ein zentrales Steuerungssystem miteinander verbunden und werden über eine gemeinsame Benutzeroberfläche bedient. Mit diesem System erhalten Sie einen Virenschutz, der sich vollständig an die Systemanforderungen Ihres internen Netzes anpassen lässt.

Kaspersky® Corporate Suite bietet Rundumschutz[2] vor Viren für:

[1] Je nach Lieferumfang

- *Computerarbeitsplätze* unter Windows 98/Me, Windows 2000/NT/XP Workstation und Linux.

- *Dateiserver* unter Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD und Linux.

- *Mailsysteme* vom Typ Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim und Qmail.

- *Internet-Firewalls*: CheckPoint Firewall –1; MS ISA Server.

- *Handheld-PCs* unter Windows CE und Palm OS.

Kaspersky® Corporate Suite beinhaltet außerdem ein zentrales Installations- und Administrationssystem, Kaspersky® Administration Kit.

Sie selbst wählen die geeigneten Virenschutzprogramme in Abhängigkeit von den in Ihrem Unternehmen verwendeten Betriebssystemen und Anwendungen.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam ist die erste in Russland entwickelte Software zum Schutz vor unerwünschten Mailings (Spam) für Unternehmen kleinerer und mittlerer Größe. Das Programm vereint moderne Verfahren der Sprachanalyse für Informationen in Textform, sämtliche modernen Verfahren zum Filtern von E-Mails (einschließlich RBL-Listen und formeller Prüfung von Nachrichten) sowie eine einmalige Auswahl an Dienstprogrammen, durch die der Nutzer in die Lage versetzt wird, bis zu 95 % der unerwünschten Nachrichten zu identifizieren und zu eliminieren.

Kaspersky® Anti-Spam ist ein Filterprogramm, das, am „Eingang“ des firmeninternen Netzwerks installiert, sämtliche eingehenden Mitteilungen auf Spam überprüft. Das Programm ist kompatibel mit jedem beliebigen Mailing-System und kann sowohl auf bereits funktionierenden als auch auf separaten Mailservern installiert werden.

Die tägliche Aktualisierung der Filterdatenbank mit Mustertexten aus unserem Sprachlabor garantiert eine hohe Effizienz dieses Produkts.

Kaspersky® Anti-Spam Personal

[2] Je nach Lieferumfang

Kaspersky® Anti-Spam **Personal** dient dem Schutz von Benutzern der Mailprogramme Microsoft Outlook und Microsoft Outlook Exchange vor unerwünschten E-Mails (Spam).

Das Softwarepaket Kaspersky Anti-Spam Personal stellt ein zuverlässiges Instrument zur Identifikation von Spam im E-Mail-Datenfluss dar, der nach den Protokollen POP3 und IMAP4 (nur für Microsoft Outlook) eingeht.

Während der Filterung werden alle möglichen Attribute eines Briefes untersucht: Absender- und Empfängeradresse, Header. Außerdem wird die *Inhaltsfilterung* angewandt, bei welcher der Inhalt des eigentlichen Briefes (einschließlich der Zeile *Betreff*) und Dateianhänge analysiert werden. Dabei werden unikale linguistische und heuristische Algorithmen verwendet.

Die tägliche automatische Aktualisierung der Filterdatenbank mit Mustertexten aus einem linguistischen Labor garantiert eine hohe Effizienz dieses Produkts.

A.2. Kontaktinformationen

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir werden Sie gern umfassend per Telefon oder E-Mail beraten.

Technischer Support	Informationen über den technischen Support finden Sie unter: **www.kaspersky.com/supportinter.html**
Allgemeine Informationen	WWW: **http://www.kaspersky.com/de/** **http://www.viruslist.com** E-Mail: **sales@kaspersky.com**

ANHANG B. INDEX

Angriffsdetektor 6, 22, 24, 69
Fenster zur Benachrichtigung über Netzwerk-Ereignis 41
Installations-CD 7
Konfigurationsfenster 21, 39, 42
Lizenzvertrag 7
Regeln für Anwendungen 21, 46
Regeln für Paketfilterung 21, 60
Sicherheitsstufen 6, 17, 21, 23, 38, 40
Skala der Sicherheitsstufen 33
Technischer Support 10
Technischer Support-Service 96

ANHANG C. HÄUFIGE FRAGEN

Bei der Ausführung einer bestimmten Aufgabe kommt es auf Ihrem Computer zu Fehlfunktionen und Sie möchten überprüfen, ob diese durch das Programm Kaspersky Anti-Hacker hervorgerufen werden.

Wählen Sie die Sicherheitsstufe **Alle erlauben** oder beenden Sie Kaspersky Anti-Hacker (entfernen Sie ihn aus dem Arbeitsspeicher). Tritt der Fehler weiterhin auf, dann steht er nicht mit der Funktion von Kaspersky Anti-Hacker in Verbindung. Sollte der Fehler weiterhin vorkommen, wenden Sie sich bitte an die Spezialisten von Kaspersky Lab.

ANHANG D. STANDARD-ENDBENUTZER-LIZENZVERTRAG

HINWEIS AN ALLE BENUTZER: BITTE LESEN SIE SORGFÄLTIG DIE FOLGENDE RECHTLICHE VEREINBARUNG ("VERTRAG") FÜR DIE LIZENZ DER ANGEGEBENEN SOFTWARE ("SOFTWARE"), DIE VON KASPERSKY LAB ("KASPERSKY LAB") HERGESTELLT WURDE.

WENN SIE DIESE SOFTWARE PER INTERNET ERWORBEN HABEN, DANN ERKLÄREN SIE (ENTWEDER ALS NATÜRLICHE ODER ALS JURISTISCHE PERSON) DURCH KLICK AUF DIE SCHALTFLÄCHE "JA" IHR EINVERSTÄNDNIS, AN DIESEN VERTRAG GEBUNDEN ZU SEIN UND ZUM VERTRAGSPARTNER ZU WERDEN. WENN SIE NICHT MIT ALLEN BESTIMMUNGEN DIESES VERTRAGES EINVERSTANDEN SIND, DANN KLICKEN SIE AUF DIE SCHALTFLÄCHE "NEIN" UND ERKLÄREN DADURCH, DASS SIE DIE VERTRAGSBESTIMMUNGEN NICHT AKZEPTIEREN UND DIE SOFTWARE NICHT INSTALLIEREN.

WENN SIE DIESE SOFTWARE AUF EINEM PHYSIKALISCHEN DATENTRÄGER ERWORBEN HABEN, DANN ERKLÄREN SIE DURCH DAS ÖFFNEN DES CD-SIEGELS IHR EINVERSTÄNDNIS, AN DIESEN VERTRAG GEBUNDEN ZU SEIN. WENN SIE NICHT MIT ALLEN BESTIMMUNGEN DIESES VERTRAGES EINVERSTANDEN SIND, ÖFFNEN SIE DAS CD-SIEGEL NICHT, FÜHREN KEINEN DOWNLOAD DURCH UND INSTALLIEREN ODER BENUTZEN DIESE SOFTWARE NICHT. SIE KÖNNEN DIESE SOFTWARE GEGEN VOLLE KOSTENERSTATTUNG ZURÜCKGEBEN. IHR RECHT AUF RÜCKGABE UND KOSTENERSTATTUNG ENDET 30 TAGE NACH DEM KAUF BEI EINEM AUTORISIERTEN KASPERSKY LAB-HÄNDLER ODER -WIEDERVERKÄUFER. DAS RECHT AUF RÜCKGABE UND KOSTENERSTATTUNG GILT NUR FÜR DEN URSPRÜNGLICHEN KÄUFER.

Jede Bezugnahme auf "SOFTWARE" schließt hierbei den Software-Aktivierungsschlüssel ("SCHLÜSSEL-IDENTIFIKATIONSDATEI") ein, der Ihnen von Kaspersky Lab als ein Teil der SOFTWARE zur Verfügung gestellt wird.

1. Lizenzgewährung. Nach erfolgter Zahlung der entsprechenden Lizenzgebühren und unter der Voraussetzung der Einhaltung der Bedingungen und Bestimmungen des VERTRAGES erteilt Kaspersky Lab Ihnen hierdurch das nicht ausschließliche und nicht übertragbare Recht zur Nutzung eines Exemplares der angegebenen Version der SOFTWARE und

der Begleitdokumentation ("DOKUMENTATION") für die Gültigkeitsdauer des VERTRAGES ausschließlich für Ihre eigenen internen Geschäftszwecke. Sie sind berechtigt, ein Exemplar der SOFTWARE auf einem Computer, einer Workstation, einem Personal Digital Assistant oder einem anderen elektronischen Hardwaregerät zu installieren, für das die SOFTWARE entwickelt wurde ("COMPUTER"). Wenn die SOFTWARE als Set oder Paket mit mehr als einem einzelnen SOFTWARE-Produkt lizenziert ist, dann erstreckt sich diese Lizenz auf jedes einzelne dieser SOFTWARE-Produkte, unter Vorbehalt aller in der entsprechenden Preisliste oder Produktverpackung genannten Einschränkungen oder Nutzungsfristen, die für jedes der SOFTWARE-Produkte einzeln gelten.

1.1 Nutzung. Die SOFTWARE ist als Einzelprodukt lizenziert. Es ist nicht gestattet, die SOFTWARE auf mehr als einem COMPUTER oder durch mehr als einen Benutzer gleichzeitig zu benutzen, mit Ausnahme der weiteren Vorschriften dieses Abschnittes.

1.1.1 Die SOFTWARE gilt als auf einem COMPUTER "benutzt", wenn sie in den Arbeitsspeicher (d.h. Random-Access-Memory oder RAM) geladen ist oder auf einem permanenten Speicher (d.h. Festplatte, CD-ROM oder andere Speichermedien) des COMPUTERS installiert wurde. Diese Lizenz berechtigt Sie, nur so viele Sicherheitskopien der SOFTWARE anzufertigen, wie für deren rechtmäßige Nutzung und ausschließlich für Backup-Zwecke nötig sind, vorausgesetzt, dass jede dieser Kopien die vollständigen Copyright-Vermerke der SOFTWARE enthält. Sie haben Aufzeichnungen über die Anzahl und den Verbleib aller Kopien der SOFTWARE und der DOKUMENTATION zu führen und alle notwendigen Vorkehrungen zum Schutz der SOFTWARE gegen unerlaubtes Kopieren oder unerlaubte Nutzung zu treffen.

1.1.2 Wenn Sie den COMPUTER, auf dem die SOFTWARE installiert ist, verkaufen, haben Sie sicherzustellen, dass vorher alle Kopien der SOFTWARE physikalisch gelöscht wurden.

1.1.3 Sie sind weder selbst berechtigt, noch dürfen Sie einer dritten Partei erlauben, einen beliebigen Teil der SOFTWARE zu dekompilieren, zurück zu entwickeln (Reverse Engineering), zu disassemblieren oder auf andere Art in von Menschen lesbare Form zu bringen. Die Interface-Informationen, die erforderlich sind, um die Kompatibilität der SOFTWARE mit unabhängig von dieser entwickelten Computerprogrammen zu erreichen, werden auf Anfrage gegen Zahlung der entsprechenden Kosten und Ausgaben für Übermittlung und Lieferung dieser Informationen von Kaspersky Lab zur Verfügung gestellt. Wenn Ihnen Kaspersky Lab mitteilt, dass es – egal aus welchen Gründen, einschließlich, aber nicht nur, Kostengründen – nicht beabsichtigt, solche Informationen zur Verfügung zu stellen, dann sind Sie berechtigt, Schritte zum Erreichen der Kompatibilität zu unternehmen,

wobei Ihnen eine Zurückentwicklung (Reverse Engineering) oder Dekompilierung nur im gesetzlich zugelassenen Umfang erlaubt ist.

1.1.4 Sie sind weder berechtigt, noch dürfen Sie einer dritten Partei erlauben, die SOFTWARE zu kopieren (außer wenn es in dieser Lizenz ausdrücklich gestattet wird), an der SOFTWARE Fehlerkorrekturen vorzunehmen oder diese anderweitig zu modifizieren, zu adaptieren oder zu übersetzen oder abgeleitete Versionen der SOFTWARE zu entwickeln.

1.1.5 Sie sind nicht berechtigt, die SOFTWARE an eine andere Person zu vermieten, zu verleasen oder zu verleihen oder Ihre Lizenzrechte auf eine andere Person zu übertragen oder Unterlizenzen zu vergeben.

1.1.6 Sie sind nicht berechtigt, diese Software in automatischen, halbautomatischen oder manuellen Tools zu verwenden, welche dazu dienen, Virensignaturen, Virenerkennungsroutinen, sowie beliebige andere Daten oder Codes zum Erkennen von schädlichem Code oder Daten zu erstellen.

1.2 Nutzung im Server-Modus. Sie dürfen die SOFTWARE nur dann auf einem COMPUTER oder auf einem Server bzw. als Server ("SERVER") innerhalb einer Multi-Nutzer- oder Netzwerk-Umgebung ("SERVER-MODUS") benutzen, wenn eine solche Nutzung in der entsprechenden Preisliste oder Produktverpackung der SOFTWARE erlaubt ist. Eine gesonderte Lizenz ist für jeden COMPUTER oder Arbeitsplatz erforderlich, der jederzeit mit dem SERVER eine Verbindung herstellen kann, ungeachtet dessen, ob solche COMPUTER oder Arbeitsplätze gleichzeitig mit der SOFTWARE verbunden sind oder tatsächlich auf die SOFTWARE zugreifen oder sie benutzen. Die Benutzung von Software oder Hardware, die die Anzahl der COMPUTER oder der Arbeitsplätze reduziert, die direkt auf die SOFTWARE zugreifen oder diese benutzen (z.B. "Multiplexing" oder "Pooling" von Software oder Hardware), verringert nicht die Anzahl der erforderlichen Lizenzen (d.h. die erforderliche Anzahl von Lizenzen entspricht der tatsächlichen Anzahl der einzelnen Eingänge in das Multiplexing oder Pooling der Software oder der Hardware). Wenn die Anzahl der COMPUTER oder der Arbeitsplätze, die mit der SOFTWARE verbunden werden können, die Anzahl der Lizenzen überschreitet, die Sie erworben haben, dann sind Sie verpflichtet, einen entsprechenden Mechanismus zu installieren, der gewährleistet, dass die Nutzung der SOFTWARE die Nutzungsgrenze nicht überschreitet, die für die von Ihnen erworbene Lizenz festgelegt ist. Diese Lizenz erlaubt Ihnen, für jeden dafür lizenzierten COMPUTER oder Arbeitsplatz jene Kopien der DOKUMENTATION anzufertigen oder herunterzuladen, die für deren rechtmäßige Nutzung notwendig sind, vorausgesetzt, dass jede dieser Kopien die vollständigen Copyright-Vermerke der DOKUMENTATION enthält.

1.3 Mehrfachlizenzen. Wenn die SOFTWARE zu Mehrfachlizenz-Bedingungen lizenziert ist, die in der entsprechenden Warenrechnung des Produkts oder in der Verpackung der SOFTWARE festgelegt sind, dann sind Sie berechtigt, die Anzahl zusätzlicher Kopien der SOFTWARE anzufertigen, zu benutzen oder zu installieren, die in den Mehrfachlizenz-Bedingungen als Anzahl der COMPUTER festgelegt ist. Sie sind verpflichtet, entsprechende Mechanismen zu installieren, um sicherzustellen, dass die Anzahl der COMPUTER, auf denen die SOFTWARE installiert wurde, die Anzahl der von Ihnen erworbenen Lizenzen nicht übersteigt. Diese Lizenz erlaubt Ihnen, für jede zusätzliche Kopie, die durch die Mehrfachlizenz autorisiert ist, eine Kopie der DOKUMENTATION anzufertigen oder herunterzuladen, vorausgesetzt, dass jede dieser Kopien die vollständigen Copyright-Vermerke der DOKUMENTATION enthält.

2. Dauer. Dieser VERTRAG ist für ein (1) Jahr gültig, es sei denn, er endet aus Gründen, die in dieser Lizenz genannt sind, früher. Der VERTRAG endet automatisch, wenn Sie eine der in dieser Lizenz festgelegten Bestimmungen, Einschränkungen oder sonstigen Bedingungen verletzen. Bei Beendigung oder Ablauf dieses VERTRAGES sind Sie verpflichtet, umgehend alle Kopien der SOFTWARE und der DOKUMENTATION zu vernichten. Sie können den VERTRAG jederzeit beenden, indem Sie alle Kopien der SOFTWARE und der DOKUMENTATION vernichten.

3. Support.

(i) Kaspersky Lab gewährleistet Ihnen für den Zeitraum eines Jahres die im Folgenden festgelegten Supportleistungen ("SUPPORTLEISTUNGEN"):

(a) nach erfolgter Zahlung der jeweils aktuellen Supportgebühr und

(b) nach vollständigem Ausfüllen des Abonnementformulars für SUPPORTLEISTUNGEN, das Ihnen mit diesem VERTRAG zur Verfügung gestellt wird oder auf der Kaspersky Lab-Webseite erhältlich ist, wobei die SCHLÜSSEL-IDENTIFIKATIONSDATEI von Ihnen verlangt werden wird, die Ihnen von Kaspersky Lab mit diesem VERTRAG übergeben wurde. Kaspersky Lab wird absolutes Stillschweigen darüber bewahren, ob Sie die Bedingung für die Bereitstellung von SUPPORTLEISTUNGEN erfüllt haben oder nicht.

(ii) Die SUPPORTLEISTUNGEN enden, wenn die jährlich erforderliche Erneuerung des Abonnements nicht erfolgt. Die Erneuerung des Abonnements erfolgt durch Bezahlung der jeweils gültigen jährlichen Supportgebühr und das erneute vollständige Ausfüllen des Abonnementformulars für SUPPORTLEISTUNGEN.

(iii) Mit dem Ausfüllen des Abonnementformulars für SUPPORTLEISTUNGEN stimmen Sie den Datenschutzbestimmungen("Privacy Policy") von Kaspersky Lab zu, die mit diesem VERTRAG verbunden sind, und Sie stimmen, wie in den Datenschutzbestimmungen festgelegt, ausdrücklich der Datenübertragung in andere Länder außerhalb Ihres eigenen Landes zu.

(iv) Unter "SUPPORTLEISTUNGEN" werden verstanden:

(a) Kostenlose Software-Updates, einschließlich Versions-Upgrades;

(b) Umfangreicher technischer Support per E-Mail und telefonischer Hotline, die vom Verkäufer und/oder Wiederverkäufer gewährleistet werden;

4. Eigentumsrechte. Die SOFTWARE ist urheberrechtlich geschützt. Alle Rechte, Titel und Interessen in und an der SOFTWARE, einschließlich aller Urheberrechte, Patente, Warenzeichen und sonstigen geistigen Eigentumsrechte liegen und verbleiben bei Kaspersky Lab und dessen Lieferanten. Der Besitz, die Installation oder der Gebrauch der SOFTWARE durch Sie überträgt keinerlei Rechte an dem geistigen Eigentum der SOFTWARE auf Sie und Sie erwerben keinerlei Rechte an der SOFTWARE, außer es ist ausdrücklich in diesem VERTRAG vorgesehen.

5. Geheimhaltung. Sie erkennen an, dass die SOFTWARE und die DOKUMENTATION, einschließlich des spezifischen Designs und der Struktur einzelner Programme und der SCHLÜSSEL-IDENTIFIKATIONS-DATEI, vertrauliche Informationen sind und Eigentum von Kaspersky Lab darstellen. Sie sind nicht berechtigt, diese vertraulichen Informationen ohne vorherige schriftliche Zustimmung von Kaspersky Lab in irgendeiner Form einer dritten Partei preiszugeben, auszuhändigen oder anderweitig zur Verfügung zu stellen. Sie haben ausreichende Sicherheitsmaßnahmen zum Schutz dieser vertraulichen Informationen zu ergreifen, und sich - ohne Einschränkung des Vorhergenannten - zu bemühen, die Sicherheit und Vertraulichkeit der SCHLÜSSEL-IDENTIFIKATIONSDATEI zu gewährleisten.

6. Gewährleistung

(i) Kaspersky Lab übernimmt für [90] Tage ab dem ersten Download oder der ersten Installation die Gewährleistung für die wesentliche in der DOKUMENTATION beschriebene Funktionalität der SOFTWARE, wenn diese richtig und wie in der DOKUMENTATION beschrieben benutzt wird.

(ii) Sie übernehmen die volle Verantwortung dafür, dass die Wahl dieser SOFTWARE Ihren Anforderungen entspricht. Kaspersky Lab übernimmt keine Gewähr dafür, dass die SOFTWARE und/oder die

DOKUMENTATION solchen Anforderungen entsprechen oder dass deren Nutzung ununterbrochen und fehlerfrei sein wird.

(iii) Der einzige Gewährleistungsanspruch von Ihrer Seite und die einzige Pflicht von Kaspersky Lab im Gewährleistungsfall nach o.g. Punkt(i) besteht nach Wahl von Kaspersky Lab entweder in der Reparatur, dem Ersatz oder der Kostenerstattung der SOFTWARE, wenn Kaspersky Lab oder seine Vertreter während der Gewährleistungsfrist darüber benachrichtigt werden. Sie haben alle Informationen zur Verfügung zu stellen, die möglicherweise erforderlich sind, um den Lieferanten bei der Lösung eines Problems mit einer defekten Komponente zu unterstützen.

(iv) Die Gewährleistung in (i) ist nicht anwendbar, wenn Sie (a) ohne Genehmigung von Kaspersky Lab irgendwelche Modifikationen an der SOFTWARE vornehmen oder vornehmen lassen, (b) die SOFTWARE in einer Weise benutzen, für die sie nicht bestimmt ist, oder (c) die SOFTWARE auf andere Art benutzen, als es durch diesen VERTRAG erlaubt ist.

(v) Die in diesem VERTRAG festgelegten Gewährleistungen und Bedingungen gelten an Stelle aller sonstigen Bedingungen, Gewährleistungen oder sonstigen Vereinbarungen, die sich auf die Lieferung oder die beabsichtigte Lieferung, das Scheitern der Lieferung oder die Verzögerung der Lieferung der SOFTWARE oder der DOKUMENTATION beziehen, welche mit Ausnahme des vorliegenden Paragraphen (v) zwischen Kaspersky Lab und Ihnen wirksam sind oder anderweitig in diesen VERTRAG oder in einen Nebenvertrag aufgenommen oder mit diesen verbunden sind, ob per Satzung, per Gesetz oder auf andere Weise, welche hiermit sämtlich ausgeschlossen werden (einschließlich, aber nicht beschränkt auf die impliziten Bedingungen, Gewährleistungen und sonstigen Vereinbarungen über zufriedenstellende Qualität, zweckdienliche Eignung oder fachgerechte und sorgfältige Nutzung).

7. Haftungsbeschränkung

(i) Die Haftung von Kaspersky Lab wird durch diesen VERTRAG für folgende Fälle nicht ausgeschlossen oder eingeschränkt: (i) Schaden durch Betrug, (ii) Tod oder Personenschaden, die durch Gesetzesverstoß, Vernachlässigung der Sorgfaltspflicht oder eine andere Nichtbeachtung einer Bestimmung dieses VERTRAGES verursacht wurden, (iii) jede Pflichtverletzung, auf die in Paragr. 12 des Sale of Goods Act von 1979 oder in Paragr. 2 des Supply of Goods and Services Act von 1982 hingewiesen wird, oder (iv) jede Haftung, die kraft Gesetzes nicht ausgeschlossen werden kann.

(ii) Der Lieferant haftet, vorbehaltlich des o.g. Punkt (i), nicht (weder vertragsrechtlich, zivilrechtlich, bei Schadensersatzklagen oder in anderen Fällen) für jedwede der folgenden Verlust- oder Schadensarten (unabhängig davon, ob ein solcher Verlust oder Schaden vorhergesehen, vorhersehbar, bekannt oder anders bedingt war):

(a) Verlust von Einkommen,

(b) Verlust von tatsächlichem oder erwartetem Gewinn (einschließlich Verlust von Gewinn aus Verträgen),

(c) Verlust aus Geldgeschäften,

(d) Verlust von erwarteten Einsparungen,

(e) Verlust eines Geschäfts,

(f) Verlust einer Gelegenheit,

(g) Verlust von Kunden,

(h) Verlust an Reputation,

(i) Verlust, Beschädigung oder Verderb von Daten oder

(j) jeden wie auch immer verursachten indirekten oder nachfolgenden Verlust oder Schaden (einschließlich eines Verlusts oder Schadens von einer in diesem Punkt (ii), (a) bis (ii), (i) genannten Art).

(iii) Die Haftung von Kaspersky Lab (ob vertragsrechtlich, zivilrechtlich, bei Schadensersatzklagen oder in anderen Fällen), die aus der Lieferung der SOFTWARE oder in Verbindung damit entsteht, beschränkt sich, vorbehaltlich Punkt(i), in jedem Falle auf den Betrag, den Sie für die SOFTWARE bezahlt haben.

8. Bei der Auslegung und Interpretation dieses VERTRAGES finden die gesetzlichen Bestimmungen von England und Wales Anwendung. Die Vertragsparteien unterliegen dabei der Rechtsprechung der Gerichte von England und Wales, außer wenn Kaspersky Lab als Kläger berechtigt ist, ein Verfahren bei einem anderen zuständigen Gericht zu beantragen.

9. (i) Dieser VERTRAG enthält die vollständigen Vereinbarungen der Vertragsparteien bezüglich des Vertragsgegenstandes und ersetzt alle, auch frühere, mündlichen oder schriftlichen Verträge, Verpflichtungen und

Versprechen zwischen Ihnen und Kaspersky Lab bezüglich des Vertragsgegenstandes, die abgeschlossen wurden oder auf die in schriftlichen oder mündlichen Verhandlungen zwischen uns oder unseren Vertretern vor diesem VERTRAG hingewiesen wurde. Alle früheren Verträge zwischen den Vertragsparteien bezüglich des Vertragsgegenstandes verlieren mit dem Tag des In-Kraft-Tretens dieses VERTRAGES ihre Gültigkeit. Mit Ausnahme der in den Punkten (ii) - (iii) vorgesehenen Fälle haben Sie keine Ansprüche hinsichtlich einer Ihnen gegenüber gemachten unwahren Aussage, auf Grund derer Sie in diesen VERTRAG eingewilligt haben ("FALSCHE DARSTELLUNG"), und Kaspersky Lab haftet ausschließlich gemäß den ausdrücklichen Bestimmungen dieses VERTRAGES.

(ii) Durch diesen VERTRAG wird die Verantwortung von Kaspersky Lab nicht für eine FALSCHE DARSTELLUNG ausgeschlossen oder eingeschränkt, die wider besseres Wissen gemacht wurde.

(iii) Die Haftung von Kaspersky Lab für eine FALSCHE DARSTELLUNG bezüglich einer zugesicherten Eigenschaft, einschließlich einer zugesicherten Eigenschaft, die die Fähigkeit des Herstellers zur Erfüllung seiner Pflichten aus diesem VERTRAG betrifft, unterliegt der Haftungsbegrenzung aus Punkt 7(iii.)